BILLS AS WELL AS VALUABLE PAPERS MOUNTING IC CHIP AND PREVENTING METHOD OF UNFAIR UTILIZATION OF THEM

Patent Number: JP2001260580

Publication date: 2001-09-25

Inventor(s): TODA YUKITOSHI

Applicant(s): HITACHI LTD

Requested Patent: JP2001260580

Application Number: JP20000077750 20000315

Priority Number(s):

IPC Classification: B42D15/10; G06F17/60; G06K17/00; G06K19/07; G06K19/00; G07D7/02

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide valuable papers, capable of preventing unfair utilization by discriminating the cheating of the same and capable of reutilizing the papers when the papers can be taken back to a regular control source, and the preventing method of unfair utilization of them. SOLUTION: A fine IC chip 104 is mounted on valuable papers 103, such as bills, stocks or the like, while the memory device of the IC chip 104 stores a lock information 511 and a lock key. The lock information 511 retains a condition of either one of lock/unlock. A business server 105 reads the condition of the lock information 511 through an IC chip reading device 407 and will not start a business process when the condition is not under the condition of unlock. A control server 101 communicates with the IC chip 104 through an IC chip reading and writing device 307 to certify that the lock key 513 is right and, thereafter, changes the condition of the lock information 511 if necessary.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-260580
(43)Date of publication of application : 25.09.2001

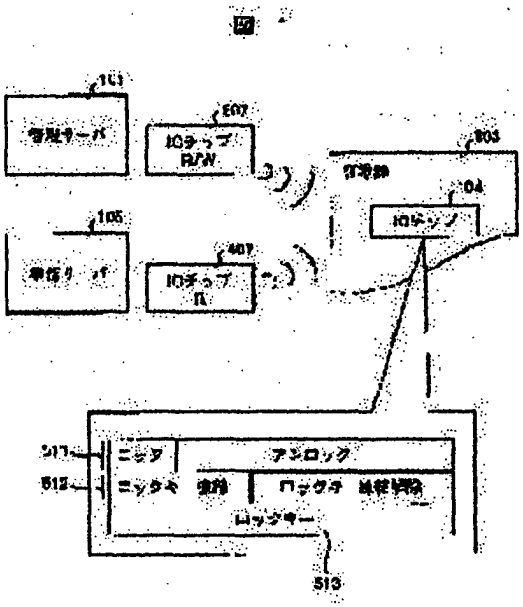
(51)Int.Cl. B42D 15/10
G06F 17/60
G06K 17/00
G06K 19/07
G06K 19/00
G07D 7/02

(21)Application number : 2000-077750
(22)Date of filing : 15.03.2000

(71)Applicant : HITACHI LTD
(72)Inventor : TODA YUKITOSHI

(54) BILLS AS WELL AS VALUABLE PAPERS MOUNTING IC CHIP AND PREVENTING METHOD OF UNFAIR UTILIZATION OF THEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide valuable papers, capable of preventing unfair utilization by discriminating the cheating of the same and capable of reutilizing the papers when the papers can be taken back to a regular control source, and the preventing method of unfair utilization of them.
SOLUTION: A fine IC chip 104 is mounted on valuable papers 103, such as bills, stocks or the like, while the memory device of the IC chip 104 stores a lock information 511 and a lock key. The lock information 511 retains a condition of either one of lock/unlock. A business server 105 reads the condition of the lock information 511 through an IC chip reading device 407 and will not start a business process when the condition is not under the condition of unlock. A control server 101 communicates with the IC chip 104 through an IC chip reading and writing device 307 to certify that the lock key 513 is right and, thereafter, changes the condition of the lock information 511 if necessary.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] They are the negotiable securities carry the IC chip carry out having the storage which stores the rewritable information which the bill which carries IC chip which can be written by non-contact, a gift certificate, a stock certificate, debentures, etc. are valuable securities, and shows whether the aforementioned IC chip can use the aforementioned securities for operating processing, and the program which can perform within the aforementioned IC chip which answers a demand from the outside and changes the aforementioned information as the feature.
[Claim 2] The bill which carries IC chip which can be written by non-contact, a gift certificate, a stock certificate, a debenture, etc. are the valuable unjust use prevention methods of securities. the aforementioned IC chip Rewritable lock/unlocking information which shows whether the aforementioned securities can be used for operating processing, Answer a demand from the outside and it has the storage which stores reference of the aforementioned lock/unlocking information, and the program which can be performed within the aforementioned IC chip which performs updating. It orders so that use of the aforementioned securities may be forbidden and the aforementioned lock/unlocking information may be set as the aforementioned IC chip by the external computer at a lock state. It orders so that use of the aforementioned securities may be enabled and the aforementioned lock/unlocking information may be set as the aforementioned IC chip by the external computer at an unlocking state. The unjust use prevention method of the negotiable securities which carry IC chip characterized by starting operating processing by the external computer with reference to the aforementioned lock/unlocking information on the aforementioned IC chip when the aforementioned lock/unlocking information is in an unlocking state.
[Claim 3] The computer of the aforementioned exterior which updates the aforementioned lock/unlocking information Save the 1st key information at the storage, and the aforementioned IC chip saves the 2nd key information which becomes the 1st key information and a pair to the storage. When it attests that the 1st key information and the 2nd key information have a predetermined correspondence relation between the computers of the aforementioned exterior and the aforementioned IC chips which update the aforementioned lock/unlocking information, The unjust use prevention method of the negotiable securities which carry IC chip according to claim 2 characterized by updating the aforementioned lock/unlocking information with the aforementioned IC chip.
[Claim 4] Valuable securities, such as a bill which is characterized by providing the following and which carries IC chip which can be written by non-contact, a gift certificate, a stock certificate, and a debenture The aforementioned IC chip is rewritable lock/unlocking information which shows whether the aforementioned securities can be used for operating processing. The negotiable securities which have the storage which stores the program which can be performed within the aforementioned IC chip which answers a demand from the outside and performs reference of the aforementioned lock/unlocking information, and updating The administrative computer which it is ordered so that the aforementioned lock/unlocking information may be updated to the aforementioned IC chip. The computer for operating processing which requires of the aforementioned IC chip, and starts operating processing with reference

to the aforementioned lock/unlocking information when the aforementioned lock/unlocking information is in an unlocking state.
[Claim 5] The aforementioned administrative computer which updates the aforementioned lock/unlocking information Save the 1st key information at the storage, and the aforementioned IC chip saves the 2nd key information which becomes the 1st key information and a pair to the storage. When it attests that the 1st key information and the 2nd key information have a predetermined correspondence relation between the aforementioned administrative computers and the aforementioned IC chips which update the aforementioned lock/unlocking information, The unjust use prevention system of the negotiable securities which carry IC chip according to claim 4 characterized by the aforementioned IC chip updating the aforementioned lock/unlocking information.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the securities set as the handling objects, such as finance / service / transportation business, and the unjust use prevention method of those. The negotiable securities which have some value, such as a bill, a gift certificate, a stock certificate, a debenture, a note, and a check, especially In case it keeps (it is only hereafter called securities) and carries, it changes into a state [that the securities unjustly acquired by the theft etc. cannot be used], or it applies to the unjust use prevention system proving the effectiveness of the securities which came to hand regularly, and is related with effective technology.
[0002]
[Description of the Prior Art] The securities showing the right which has various value as it is as promising payment of money **** [„ and] are circulating in the world. [carrying out payment of transactions conventionally] [exchanging goods] [financing incorporated company] [promising payment of OK and price by a third person to the business fund]
[0003] Although a safe, a trunk, etc. which a physical key requires are locked, or it stations a guard in order to prevent a theft in keeping these securities temporarily or carrying them, it does not carry out adding a certain processing to especially securities, but the present condition is in the state which can be used as it is.
[0004] In addition, since the uninhabited ATM/CD terminal put on the street may be destroyed in recent years using a heavy industrial machine called a power shovel etc. and the cash currently kept may be squeezed, when malfeasances, such as destruction, are committed to a ATM/CD terminal, there is technology of describing the fact which sprayed ink on the bill and suited the theft.
[0005]
[Problem(s) to be Solved by the Invention] There are the following problems in this conventional method. That is, the securities which once suited the theft are in the state where what is used regularly, and distinction do not stick, it is used unjustly, or marks, such as ink, are attached, and it has the problem that it is not reusable even if a just owner can recover. Moreover, it may not be certainly attached to the total of the securities out of which ink is squeezed.
[0006] It is in offering the securities which can be reused when the purpose of this invention solves the above-mentioned problem, and the unjust use of securities by which the theft was carried out is prevented or it recovers to regular management origin, and the unjust use prevention method of those.
[0007]
[Means for Solving the Problem] this invention makes it identifiable whether it is what may be used as what could not read the information on IC chip carried in securities about the securities kept or conveyed, and could not use as what was squeezed unjustly, or was transferred regularly.
[0008] In this invention, in order to discriminate the propriety of use of securities, it carries out by registering the identification information of use propriety into IC chip carried in securities. Recent years come and development of IC chip (RFID) of the non-contact communication formula of several mm (2-

3mm) angle has been announced for size by the newspaper etc. If such detailed IC chip manufacturing technologies progress further, IC chip with which a bill, negotiable securities, etc. can be equipped will appear. every one sheet of the securities as used in the field of [this invention / thin media, such as such papers, / detailed IC chip] this invention -- carrying -- the securities concerned -- the information on each effectiveness is given and it makes it possible to read and discriminate those information

[0009] It is possible per management of the corporation or place of business which manages storage/conveyance, and, as for the R/W to IC chip carried in securities, the security about the writing of the information on IC chip also manages the securities concerned. Therefore, when the others squeeze the securities which regular management origin keeps or carries, By showing that it is in a state [that the information on IC chip carried in the securities concerned cannot use], and reading this information to the utilization time of securities It becomes possible by being able to discriminate that the securities concerned are squeezed unjustly and refusing to use these in this state to prevent unjust use. In case reading of the information on IC chip carried in securities uses securities for operating processing, it enables it to read it by IC chip reader.

[0010] The writing of the information on IC chip carried in securities enables it for the control information for security (a personal identification number, cryptographic key, etc.) to, perform only the administrative computer holding such control information on the other hand, and the third person who does not know control information prevents from rewriting the information on IC chip.

[0011] Moreover, new management origin can change to the control information to manage by canceling a rewriting limit of control information using the control information which old management origin had set up so that it may change into original control information required in order that new management origin may rewrite the information on IC chip carried in the securities it is incomparable for the candidate for transfer, in transferring regularly the management of the securities which a certain management origin manages to another management origin. In this way, new management origin can rewrite now the information on IC chip carried in securities using the security control information under its management if needed.

[0012] Therefore, if the securities once squeezed unjustly can be returned to management origin with the just security control information which can rewrite the information on the original IC chip, it can be returned to the state where the information on IC chip of securities which was use improper can be used, and can be reused satisfactory.

[0013] Since the information on the use propriety of securities can be certainly written as mentioned above about the management unit total which carried IC chip by non-contact communication according to the securities and the unjust use prevention method of those of this invention, if the squeezed securities can be discriminated, the unjust use can be prevented and it returns to a still more regular owner's hand, returning to the state which can be used again is also possible.

[0014]

[Embodiments of the Invention] Unjust use prevention of securities is explained using a drawing about the operation form made possible below.

[0015] Drawing 1 is drawing showing the outline composition of this operation form. Securities 103 are equipped with the detailed IC chip 104. Securities 103 are equipped with the IC chip 104 by the method of pasting up the seal which became empty among two sheets of papers which constitute securities 103, or enclosed the IC chip 104 on securities 103. Anyway, securities 103 are equipped with the IC chip 104 by the method which cannot pull apart the IC chip 104 from securities 103, without damaging so that securities 103 are made unusable. The lock information 511, the lock key freeze information 512, and a lock key 513 are recorded on the storage in the IC chip 104. The lock information 511 has the state of a lock state or an unlocking state. A lock state is in the state where securities 103 cannot be used because of operating processing, and an unlocking state is in the state where securities 103 can be used because of operating processing. A lock key 513 is a bit string used as keys (a password, cryptographic key, etc.) required in order to change the lock information 511, the lock key freeze information 512, and lock key 513 the very thing. The lock key freeze information 512 has the state of a lock key freeze state or a lock key freeze release state. A lock key freeze state is in the state which cannot freeze and update a lock key

513, and a lock key freeze release state is in the state which can update a lock key 513.
[0016] The management server 101 has the authority to update the lock information 511, the lock key freeze information 512, and a lock key 513, is a computer which manages a lock key 513, and connects IC chip reading and write-in equipment 307. The management server 101 reads the information on the IC chip 104 carried in securities 103 through IC chip reading and write-in equipment 307 by non-contact, and performs change of the lock information 511, change of the lock key freeze information 512, and renewal of a lock key 513.
[0017] The operating server 105 is a computer which performs operating processing about securities 103, and connects IC chip reader 407. The operating server 105 accesses the lock information 511 on the IC chip 104 of securities 103 through IC chip reader 407, if the lock information 511 is in an unlocking state, it will perform operating processing which deals with securities 103, and if it is in a lock state, it will not perform operating processing.
[0018] Drawing 2 is drawing explaining the example of the procedure of using the securities 103 equipped with the IC chip 104. The securities 103 equipped with the IC chip 104 shall be the securities 103 which entered from the manufacture process of securities 103, it shall be used first, and shall be managed by other management servers, or shall go into the bottom of management of the management server 101 concerned first, and the lock information 511 shall be in a lock state and the state of a lock key freeze of the lock key freeze information 512.
[0019] Drawing 2 (a) is a step updated to the lock key to which the management server 101 carries out lock key freeze release of the lock key freeze information 512 about the IC chip 104 on securities 103, and he manages a lock key 513. Drawing 2 (b) is a step at which the management server 101 changes the lock information 511 into a lock state about the IC chip 104 on securities 103, and changes the lock key freeze information 512 into the state of a lock key freeze. Drawing 2 (c) shows the step which keeps or carries the securities 103 of this state. The securities 103 of this state cannot be used for operating processing. Moreover, a lock key 513 cannot be unfairly updated to the lock key under its management by other management servers.
[0020] Drawing 2 (d) is a step at which the management server 101 changes the lock information 511 into the state of unlocking about the IC chip 104 on securities 103, in order to use these securities 103 for operating processing. In drawing 2 (e), the operating server 105 accesses the lock information 511 on the IC chip 104 on securities 103, and checks the propriety of use. If the lock information 511 is in an unlocking state, the operating processing about these securities 103 will be started, and if the lock information 511 is in a lock state, operating processing about these securities 103 will not be performed. Therefore, operating processing of the securities 103 which met the theft etc. during storage or conveyance is not carried out.
[0021] It is transferred to another financial institution from the financial institution which has securities 103 as moving from under management of the management server which has the above-mentioned securities 103 to the bottom of management of another management server, or the case where it is transferred between places of business is assumed. Therefore, as long as the problem of security does not arise, unlocking and the lock key freeze information 512 may transfer [the lock information 511 on the IC chip 104] securities 103 between places of business in the state of lock key freeze release.
[0022] Drawing 3 is drawing showing the outline composition of the management server 101. As shown in drawing 3 , the management server 101 has CPU301, memory 302, a magnetic disk unit 303, keyboard equipment 304, a display unit 305, CD-ROM equipment 306, and IC chip reading and write-in equipment 307. The magnetic disk unit 303 stores the lock key managed table 308. The whole management server 101 may be a pocket information processor.
[0023] CPU301 is equipment which controls operation of the management server 101 whole. Memory 302 is storage which stores various processing programs and data. A magnetic disk unit 303 is storage which stores various processing programs and data. Keyboard equipment 304 is equipment for a data input, and a display unit 305 is equipment which displays various data. CD-ROM equipment 306 is equipment which reads the contents of CD-ROM which recorded various processing programs. IC chip reading and write-in equipment 307 are equipment which write information by non-contact between the

IC chips 104 carried in securities 103.
[0024] The lock key managed table 308 is a table which stores the lock key which the management server 101 concerned manages.
[0025] A lock / lock key processing section 310 is stored in memory 302, as shown in drawing 2 , it is a program which performs processing concerning management of the lock information 511 recorded on the IC chip 104 of securities 103, the lock key freeze information 512, and a lock key 513, and it is performed by CPU301.
[0026] After storing in magnetic-disk-unit 303 grade the lock / lock key processing section 310 recorded on record media, such as CD-ROM, it shall load to memory 302 and shall perform. In addition, other record media other than CD-ROM may be used as a record medium which records this program.
[0027] Drawing 4 is drawing showing the outline composition of the operating server 105. As shown in drawing 4 , the operating server 105 has CPU401, memory 402, a magnetic disk unit 403, keyboard equipment 404, a display unit 405, CD-ROM equipment 406, and IC chip reader 407.
[0028] CPU401 is equipment which controls operation of the operating server 105 whole. Memory 402 is storage which stores various processing programs and data. A magnetic disk unit 403 is storage which stores various processing programs and data. IC chip reader 407 is equipment which reads the lock information 511 in the IC chip 104 carried in securities 103 by non-contact.
[0029] Memory 402 stores the lock judging processing section 410 and the operating processing section 411. The lock judging processing section 410 is a program which performs processing which reads the lock information 511 on the IC chip 104 carried in securities 103, and judges the propriety of use of the securities 103 concerned. It is the processing section which processes operating application about the securities 103 judged that the operating processing section 411 can be used.
[0030] After storing in magnetic-disk-unit 403 grade the program containing the lock judging processing section 410 recorded on record media, such as CD-ROM, it shall load to memory and shall perform. In addition, other record media other than CD-ROM may be used as a record medium which records this program.
[0031] Drawing 5 is drawing showing the internal configuration of the IC chip 104 carried in securities 103. The IC chip 104 is a detailed semiconductor chip, and as shown in drawing 5 , it has the communication antenna 501, electromagnetic-induction electromotive equipment 502, power accumulation equipment 503, a control unit 504, and storage 505.
[0032] The communication antenna 501 is equipment which transmits and receives information between the IC chip 104, IC chip reading and write-in equipment 307, or IC chip reader 407, or receives the electromagnetic wave for the electric power supply used as the power supply which drives the IC chip 104 from IC chip reading and write-in equipment 307, or IC chip reader 407. Electromagnetic-induction electromotive equipment 502 is equipment which transforms into power the electromagnetic wave received with the communication antenna 501 by electromagnetic induction. Power accumulation equipment 503 is equipment used as the power supply for accumulating the power which carried out electromotive with electromagnetic-induction electromotive equipment 502, and driving the IC chip 104.
[0033] A control unit 504 is equipment which controls operation of the IC chip 104 whole including a microprocessor. Storage 505 stores various programs, such as the lock information 511, the lock key freeze information 512 and management information of a lock key 513, the code decode program 521 and the lock key right-or-wrong judging program 522, the renewal program 523 of lock state reference, and the renewal program 524 of a lock key.
[0034] The lock information 511 stores the 1-bit information which shows the state of a lock/unlocking. The lock key freeze information 512 stores the 1-bit information which shows a lock key freeze / lock key freeze release. A lock key 513 is information managed as a key given to the IC chip 104 concerned.
[0035] Drawing 6 is drawing explaining the state transition of the lock information 511 recorded on the IC chip 104, and the lock key freeze information 512. The state of the lock information 511 and the lock key freeze information 512 has three, the state 601 of a lock and a lock key freeze, the state 602 of unlocking and a lock key freeze, and the state 603 of unlocking and lock key freeze release.

[0036] A state 601 is in the state which cannot use the securities 103 concerned and cannot update a lock key 513. It can change in the state 602 from a state 601 by using the right lock key.
[0037] A state 602 can use the securities 103 concerned, and is in the state which cannot update a lock key 513. It can change in the state 603 from a state 602 by using the right lock key. Moreover, it can change in the state 601 from a state 602 by using the right lock key.
[0038] A state 603 can use the securities 103 concerned, and is in the state which can update a lock key 513. It can change in the state 602 from a state 603 by using the right lock key.
[0039] Drawing 7 A and drawing 7 B are flow charts which show the flow of processing of the lock / lock key processing section 310 of the management server 101. A lock / lock key processing section 310 receives the demand inputted from the keyboard etc. about the target securities 103 (Step 701). a demand is shown below -- there are four kinds (1) Change into a lock state the lock information 511 on the IC chip 104 carried in the securities 103 concerned from an unlocking state. (2) Change the lock information 511 into an unlocking state from a lock state. Whether the lock key freeze information 512 is changed into a lock key freeze state or it changes into the state of lock key freeze release need to be specified of this demand. (3) Update a lock key 513 after changing an unlocking state and the lock key freeze information 512 into a lock key freeze release state for the lock information 511. (4) Change a lock state and the lock key freeze information 512 into a lock key freeze state for the lock information 511 after updating a lock key 513.
[0040] Next, a lock / lock key processing section 310 judges whether the lock key registered into the lock key or the lock key managed table 308 which is the lock key which received the notice from old management origin, and was inputted from the keyboard 304 etc., and the lock key 513 on the IC chip 104 are in agreement in whether a lock key 513 is right (Step 702). Since the lock key 513 is not updated yet here, it will collate about the lock key before renewal of a lock key, and the lock key is either of the lock keys which received the notice from the lock key which the management server 101 concerned manages, or other management places of business. If a lock key 513 is not right (Step 702, error), it considers as a processing end.
[0041] If a lock key 513 is right, unlocking processing which changes the lock information 511 on the IC chip 104 concerned into an unlocking state will be performed (Step 703). Next, if renewal of a lock key is not demanded (Step 704), it goes to Step 709. When renewal of a lock key is demanded, it judges whether a lock key 513 is right (Step 705). Here, the check of Step 702 will be repeated and it is judged with a lock key 513 being right. Next, the lock key freeze information 512 is read, and if it is in a lock key freeze state (Step 706, freeze), this will be changed into the state of lock key freeze release (Step 707). Next, with reference to the lock key managed table 308, the lock key 513 on the IC chip 104 is updated to the new lock key under management of the management server 101 (Step 708).
[0042] Next, it moves to drawing 7 B and judges whether a lock / lock key processing section 310 freezes a lock key (Step 709). When specification of a lock key freeze is carried out by a demand (1), (4), and (2), the freeze of a lock key is required. In not carrying out a lock key freeze, it goes to Step 712. Next, it judges whether a lock key 513 is right (Step 710). When renewal of a lock key of Step 708 is carried out, coincidence with the lock key on the lock key managed table 308 and the lock key 513 after updating is judged, and it is judged with naturally a lock key 513 being right. When renewal of a lock key of Step 708 has not been carried out, the check of Step 702 will be repeated and it is judged with a lock key 513 being right. if a lock key is right (Step 710 -- right), the lock key freeze information 512 will be changed into a lock key freeze state (Step 711)
[0043] Next, it judges whether a lock / lock key processing section 310 changes the lock information 511 into a lock state (Step 712). It is necessary to change the lock information 511 into a lock state about a demand (1) and (4). In locking (Step 712), it judges whether a lock key 513 is right again (Step 713). The check of Step 702 and Step 710 will be repeated at a demand (1) and the case of (4), and it is judged with a lock key 513 being right. if a lock key is right (Step 713 -- right), the lock key freeze information 512 is in the state of a freeze (Step 714, freeze), and when the lock information 511 is in an unlocking state, (Step 715, unlocking), and lock processing that changes the lock information 511 into a lock state will be performed (Step 716)

[0044] When the lock key freeze information 512 which is contradictory to the judgment of Step 709 at Step 714 when there is an error of a lock key at Step 710, it does not lock at Step 712 and there is an error of a lock key at Step 713 is in a lock key freeze release state, and when the lock information 511 is in a lock state at Step 715, it considers as a processing end immediately.
[0045] Although the check with a right lock key 513 was based on the judgment with the lock key which suited under another management or the lock key on the lock key managed table 308, and the lock key 513 in agreement on the IC chip 104 with the above-mentioned operation gestalt If a lock key with a plaintext is transmitted to the IC chip 104 or a lock key with a plaintext is transmitted to it from the IC chip 104 through IC chip reading and write-in equipment 307 to the management server 101 from the management server 101, the danger that security will be broken will become high. For example, if the electromagnetic wave sent out from IC chip reading and write-in equipment 307 is intercepted, the lock key transmitted between the management server 101 and the IC chip 104 can be known. In order to avoid such risk, it is desirable to transmit the numeric value which made the lock key the cryptographic key, without transmitting a direct lock key, and was enciphered by the lock key. For example, the random number which enciphered the random number which used as the public key the lock key registered into the lock key managed table 308, and a lock / lock key processing section 310 made generate a random number, and was generated with this public key, and was enciphered, and the original random number are transmitted to the IC chip 104. The lock key right-or-wrong judging program 522 of the IC chip 104 When the command of a lock key right-or-wrong judging is received, the random number with which the code decode program 521 was enciphered by the lock key 513 saved as a private key is decoded. It is able for the lock key right-or-wrong judging program 522 to compare with the original random number the random number by which decode was carried out, to judge the right or wrong of a lock key, and to notify the result (positive or no) to the lock / lock key processing section 310 of the management server 101. In this case, the lock key which suited under another management or the lock key on the lock key managed table 308, and the lock key 513 on the IC chip 104 have the correspondence relation of a public key pair, and, generally the same value does not become. Therefore, the lock key which can generally creep and is under that management, and the lock key 513 on the IC chip 104 do not need to be the same values, and should just be the numeric value which had a predetermined correspondence relation.
[0046] finishing [the renewal program 523 of lock state reference on the IC chip 104 / a judgment of the right or wrong of a lock key] when the command which requires reference of the lock information 511 is received from the management server 101 or the operating server 105 -- it is -- it is not involved nothing but transmits to content of lock information 511 demand-origin However, this demand will not be answered if it is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires renewal of the lock information 511 is received. Moreover, if the renewal program 523 of lock state reference is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires the reference or updating of the lock key freeze information 512 is received, it will not answer this demand.
[0047] Similarly, if the renewal program 524 of a lock key on the IC chip 104 is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires renewal of a lock key 513 is received, it will not answer this demand. In using a public key pair as a lock key, after transmitting the updating demand command of a lock key 513 to the IC chip 104 and obtaining a response, a lock / lock key processing section 310 enciphers the lock key after updating (private key) by the old lock key (public key), and transmits to the IC chip 104. The renewal program 524 of a lock key is decoded by the old lock key (private key) in which the encryption information received through the code decode program 521 is stored by the lock key 513, and transposes a lock key 513 to the new lock key (private key) by which decode was carried out. In using a common key instead of a public key pair as a lock key, a lock / lock key processing section 310 enciphers a new lock key (common key) by the old lock key (common key) similarly, it transmits to the IC chip 104, the encryption information which the renewal program 524 of a lock key received is decoded by the old lock key (common key), and it transposes to the lock key which was able to obtain the lock key 513.

[0048] The lock key right-or-wrong judging program 522 has a lock key right-or-wrong judging flag on storage 505, and saves the result (positive or no) of a right-or-wrong judging of a lock key. And this lock key right-or-wrong judging flag is reset to an initial state (no) at the time of each processing end of processing (unlocking processing) of Step 703, processing (renewal of a lock key) of Step 708, processing (freezing treatment of a lock key) of Step 711, and processing (lock processing) of Step 716. In any [of demand (1) - (4)] case, this flag is reset by the state of no by such composition at the time of a processing end.
[0049] In addition, although the lock key freeze information 512 was formed in the IC chip 104, and updating of a lock key 513 was enabled with the above-mentioned operation form only when the lock key freeze information 512 was in a lock key freeze release state, the lock key freeze information 512 is not established, but when a lock key is right irrespective of the state of the lock information 511, this invention can be carried out also in the form which degenerated so that lock key 513 updating might always be enabled. In this case, a demand becomes three kinds of (1) and (2), (3), or (4), and processing of Steps 706, 707,709,710,711, and 714 is excepted.
[0050] Moreover, an identification number (ID) like the serial number of the IC chip 104 concerned may be given to the storage 505 of the IC chip 104, the correspondence table of this ID and lock key may be prepared in the lock key managed table 308, and the securities 103 which carried the IC chip 104 by the pair of ID and a lock key may be managed. Moreover, if it is used in order to only call the IC chip 104 theft prevention under storage or transportation, the management server 101 is able to give and manage the same lock key for the IC chip 104 of all the securities 103 put under management. Only as for the management server 101 concerned, the securities 103 which carry the IC chip 104 set in the lock state recovered from the theft etc. change into the state of unlocking.
[0051] Or if the value which shows the invalid of the lock key 513 beforehand specified specially to the lock information 511 on the IC chip 104 as a modification about the above-mentioned operation form is set up and it will be made the structure which cannot return to an unlocking state eternally, electronic abandonment processing can be given to the securities of this invention the same with carrying out decision (abandonment) processing so that the reuse of the gift certificate after use cannot be carried out, for example etc.
[0052] What is necessary is just to opt for the function of the program which is the balance of the required grade of security, and the cost of the IC chip 104, and stores in the hardware of the IC chip 104, and the IC chip 104, and the IC chip 104 performs since various deformation can be performed in operation of this invention like described above.
[0053] It is possible to judge from the information on IC chip carried in the securities concerned, to perform operating processing justly or to prevent unjust use as mentioned above, without an operating server asking a management server the propriety of the execution of operating processing to the securities concerned by the online network etc. with this operation form. Moreover, the method of this invention is applied, and the reuse can be enabled when the once squeezed securities which cannot be used are able to be regained under management of a just management server.
[0054] Since the propriety of use of the securities concerned can be judged using the information on IC chip carried in securities according to this operation form as explained above, it is possible to discriminate on that spot whether they are the securities squeezed unjustly, and to prevent unjust use.
[0055]
[Effect of the Invention] It is possible to return to the state which can be reused when unjust use can be prevented and it is able to return to just management origin, since the securities unjustly squeezed using the information on IC chip carried in securities were discriminable according to this invention.

[Translation done.]

* NOTICES *

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[The technical field to which invention belongs] This inventions are negotiable securities which have some value, such as a bill, a gift certificate, a stock certificate, a debenture, a note, and a check, especially with respect to the securities set as the handling objects, such as finance / service / transportation business, and the unjust use prevention method of those. In case it keeps (it is only hereafter called securities) and carries, it changes into a state [that the securities unjustly acquired by the theft etc. cannot be used], or it applies to the unjust use prevention system proving the effectiveness of the securities which came to hand regularly, and is related with effective technology.

[Translation done.]

* NOTICES *

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. * ** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] The securities showing the right which has various value as it is as promising payment of money **** [„ and] are circulating in the world. [carrying out payment of transactions conventionally] [exchanging goods] [financing incorporated company] [promising payment of OK and price by a third person to the business fund]
[0003] Although a safe, a trunk, etc. which a physical key requires are locked, or it stations a guard in order to prevent a theft in keeping these securities temporarily or carrying them, it does not carry out adding a certain processing to especially securities, but the present condition is in the state which can be used as it is.
[0004] In addition, since the uninhabited ATM/CD terminal put on the street may be destroyed in recent years using a heavy industrial machine called a power shovel etc. and the cash currently kept may be squeezed, when malfeasances, such as destruction, are committed to a ATM/CD terminal, there is technology of describing the fact which sprayed ink on the bill and suited the theft.

[Translation done.]

* NOTICES *

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] It is possible to return to the state which can be reused when unjust use can be prevented and it is able to return to just management origin, since the securities unjustly squeezed using the information on IC chip carried in securities were discriminable according to this invention.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] There are the following problems in this conventional method. That is, the securities which once suited the theft are in the state where what is used regularly, and distinction do not stick, it is used unjustly, or marks, such as ink, are attached, and it has the problem that it is not reusable even if a just owner can recover. Moreover, it may not be certainly attached to the total of the securities out of which ink is squeezed.
[0006] It is in offering the securities which can be reused when the purpose of this invention solves the above-mentioned problem, and the unjust use of securities by which the theft was carried out is prevented or it recovers to regular management origin, and the unjust use prevention method of those.

[Translation done.]

MEANS

[Means for Solving the Problem] this invention makes it identifiable whether it is what may be used as what could not read the information on IC chip carried in securities about the securities kept or conveyed, and could not use as what was squeezed unjustly, or was transferred regularly.
[0008] In this invention, in order to discriminate the propriety of use of securities, it carries out by registering the identification information of use propriety into IC chip carried in securities. Recent years come and development of IC chip (RFID) of the non-contact communication formula of several mm (2-3mm) angle has been announced for size by the newspaper etc. If such detailed IC chip manufacturing technologies progress further, IC chip with which a bill, negotiable securities, etc. can be equipped will appear. every one sheet of the securities as used in the field of [this invention / thin media, such as such papers, / detailed IC chip] this invention -- carrying -- the securities concerned -- the information on each effectiveness is given and it makes it possible to read and discriminate those information
[0009] It is possible per management of the corporation or place of business which manages storage/conveyance, and, as for the R/W to IC chip carried in securities, the security about the writing of the information on IC chip also manages the securities concerned. Therefore, when the others squeeze the securities which regular management origin keeps or carries, By showing that it is in a state [that the information on IC chip carried in the securities concerned cannot use], and reading this information to the utilization time of securities It becomes possible by being able to discriminate that the securities concerned are squeezed unjustly and refusing to use these in this state to prevent unjust use. In case reading of the information on IC chip carried in securities uses securities for operating processing, it enables it to read it by IC chip reader.
[0010] The writing of the information on IC chip carried in securities enables it for the control information for security (a personal identification number, cryptographic key, etc.) to, perform only the administrative computer holding such control information on the other hand, and the third person who does not know control information prevents from rewriting the information on IC chip.
[0011] Moreover, new management origin can change to the control information to manage by canceling a rewriting limit of control information using the control information which old management origin had set up so that it may change into original control information required in order that new management origin may rewrite the information on IC chip carried in the securities it is incomparable for the candidate for transfer, in transferring regularly the management of the securities which a certain management origin manages to another management origin. In this way, new management origin can rewrite now the information on IC chip carried in securities using the security control information under its management if needed.
[0012] Therefore, if the securities once squeezed unjustly can be returned to management origin with the just security control information which can rewrite the information on the original IC chip, it can be returned to the state where the information on IC chip of securities which was use improper can be used, and can be reused satisfactory.
[0013] Since the information on the use propriety of securities can be certainly written as mentioned above about the management unit total which carried IC chip by non-contact communication according

to the securities and the unjust use prevention method of those of this invention, if the squeezed securities can be discriminated, the unjust use can be prevented and it returns to a still more regular owner's hand, returning to the state which can be used again is also possible.
[0014]
[Embodiments of the Invention] Unjust use prevention of securities is explained using a drawing about the operation gestalt made possible below.
[0015] Drawing 1 is drawing showing the outline composition of this operation gestalt. Securities 103 are equipped with the detailed IC chip 104. Securities 103 are equipped with the IC chip 104 by the method of pasting up the seal which became empty among two sheets of papers which constitute securities 103, or enclosed the IC chip 104 on securities 103. Anyway, securities 103 are equipped with the IC chip 104 by the method which cannot pull apart the IC chip 104 from securities 103, without damaging so that securities 103 are made unusable. The lock information 511, the lock key freeze information 512, and a lock key 513 are recorded on the storage in the IC chip 104. The lock information 511 has the state of a lock state or an unlocking state. A lock state is in the state where securities 103 cannot be used because of operating processing, and an unlocking state is in the state where securities 103 can be used because of operating processing. A lock key 513 is a bit string used as keys (a password, cryptographic key, etc.) required in order to change the lock information 511, the lock key freeze information 512, and lock key 513 the very thing. The lock key freeze information 512 has the state of a lock key freeze state or a lock key freeze release state. A lock key freeze state is in the state which cannot freeze and update a lock key 513, and a lock key freeze release state is in the state which can update a lock key 513.
[0016] The management server 101 has the authority to update the lock information 511, the lock key freeze information 512, and a lock key 513, is a computer which manages a lock key 513, and connects IC chip reading and write-in equipment 307. The management server 101 reads the information on the IC chip 104 carried in securities 103 through IC chip reading and write-in equipment 307 by non-contact, and performs change of the lock information 511, change of the lock key freeze information 512, and renewal of a lock key 513.
[0017] The operating server 105 is a computer which performs operating processing about securities 103, and connects IC chip reader 407. The operating server 105 accesses the lock information 511 on the IC chip 104 of securities 103 through IC chip reader 407, if the lock information 511 is in an unlocking state, it will perform operating processing which deals with securities 103, and if it is in a lock state, it will not perform operating processing.
[0018] Drawing 2 is drawing explaining the example of the procedure of using the securities 103 equipped with the IC chip 104. The securities 103 equipped with the IC chip 104 shall be the securities 103 which entered from the manufacture process of securities 103, it shall be used first, and shall be managed by other management servers, or shall go into the bottom of management of the management server 101 concerned first, and the lock information 511 shall be in a lock state and the state of a lock key freeze of the lock key freeze information 512.
[0019] Drawing 2 (a) is a step updated to the lock key to which the management server 101 carries out lock key freeze release of the lock key freeze information 512 about the IC chip 104 on securities 103, and he manages a lock key 513. Drawing 2 (b) is a step at which the management server 101 changes the lock information 511 into a lock state about the IC chip 104 on securities 103, and changes the lock key freeze information 512 into the state of a lock key freeze. Drawing 2 (c) shows the step which keeps or carries the securities 103 of this state. The securities 103 of this state cannot be used for operating processing. Moreover, a lock key 513 cannot be unfairly updated to the lock key under its management by other management servers.
[0020] Drawing 2 (d) is a step at which the management server 101 changes the lock information 511 into the state of unlocking about the IC chip 104 on securities 103, in order to use these securities 103 for operating processing. In drawing 2 (e), the operating server 105 accesses the lock information 511 on the IC chip 104 on securities 103, and checks the propriety of use. If the lock information 511 is in an unlocking state, the operating processing about these securities 103 will be started, and if the lock

information 511 is in a lock state, operating processing about these securities 103 will not be performed. Therefore, operating processing of the securities 103 which met the theft etc. during storage or conveyance is not carried out.

[0021] It is transferred to another financial institution from the financial institution which has securities 103 as moving from under management of the management server which has the above-mentioned securities 103 to the bottom of management of another management server, or the case where it is transferred between places of business is assumed. Therefore, as long as the problem of security does not arise, unlocking and the lock key freeze information 512 may transfer [the lock information 511 on the IC chip 104] securities 103 between places of business in the state of lock key freeze release.

[0022] Drawing 3 is drawing showing the outline composition of the management server 101. As shown in drawing 3 , the management server 101 has CPU301, memory 302, a magnetic disk unit 303, keyboard equipment 304, a display unit 305, CD-ROM equipment 306, and IC chip reading and write-in equipment 307. The magnetic disk unit 303 stores the lock key managed table 308. The whole management server 101 may be a pocket information processor.

[0023] CPU301 is equipment which controls operation of the management server 101 whole. Memory 302 is storage which stores various processing programs and data. A magnetic disk unit 303 is storage which stores various processing programs and data. Keyboard equipment 304 is equipment for a data input, and a display unit 305 is equipment which displays various data. CD-ROM equipment 306 is equipment which reads the content of CD-ROM which recorded various processing programs. IC chip reading and write-in equipment 307 are equipment which write information by non-contact between the IC chips 104 carried in securities 103.

[0024] The lock key managed table 308 is a table which stores the lock key which the management server 101 concerned manages.

[0025] A lock / lock key processing section 310 is stored in memory 302, as shown in drawing 2 , it is a program which performs processing concerning management of the lock information 511 recorded on the IC chip 104 of securities 103, the lock key freeze information 512, and a lock key 513, and it is performed by CPU301.

[0026] After storing in magnetic-disk-unit 303 grade the lock / lock key processing section 310 recorded on record media, such as CD-ROM, it shall load to memory 302 and shall perform. In addition, other record media other than CD-ROM may be used as a record medium which records this program.

[0027] Drawing 4 is drawing showing the outline composition of the operating server 105. As shown in drawing 4 , the operating server 105 has CPU401, memory 402, a magnetic disk unit 403, keyboard equipment 404, a display unit 405, CD-ROM equipment 406, and IC chip reader 407.

[0028] CPU401 is equipment which controls operation of the operating server 105 whole. Memory 402 is storage which stores various processing programs and data. A magnetic disk unit 403 is storage which stores various processing programs and data. IC chip reader 407 is equipment which reads the lock information 511 in the IC chip 104 carried in securities 103 by non-contact.

[0029] Memory 402 stores the lock judging processing section 410 and the operating processing section 411. The lock judging processing section 410 is a program which performs processing which reads the lock information 511 on the IC chip 104 carried in securities 103, and judges the propriety of use of the securities 103 concerned. It is the processing section which processes operating application about the securities 103 judged that the operating processing section 411 can be used.

[0030] After storing in magnetic-disk-unit 403 grade the program containing the lock judging processing section 410 recorded on record media, such as CD-ROM, it shall load to memory and shall perform. In addition, other record media other than CD-ROM may be used as a record medium which records this program.

[0031] Drawing 5 is drawing showing the internal configuration of the IC chip 104 carried in securities 103. The IC chip 104 is a detailed semiconductor chip, and as shown in drawing 5 , it has the communication antenna 501, electromagnetic-induction electromotive equipment 502, power accumulation equipment 503, a control unit 504, and storage 505.

[0032] The communication antenna 501 is equipment which transmits and receives information between

the IC chip 104, IC chip reading and write-in equipment 307, or IC chip reader 407, or receives the electromagnetic wave for the electric power supply used as the power supply which drives the IC chip 104 from IC chip reading and write-in equipment 307, or IC chip reader 407. Electromagnetic-induction electromotive equipment 502 is equipment which transforms into power the electromagnetic wave received with the communication antenna 501 by electromagnetic induction. Power accumulation equipment 503 is equipment used as the power supply for accumulating the power which carried out electromotive with electromagnetic-induction electromotive equipment 502, and driving the IC chip 104.

[0033] A control unit 504 is equipment which controls operation of the IC chip 104 whole including a microprocessor. Storage 505 stores various programs, such as the lock information 511, the lock key freeze information 512 and management information of a lock key 513, the code decode program 521 and the lock key right-or-wrong judging program 522, the renewal program 523 of lock state reference, and the renewal program 524 of a lock key.

[0034] The lock information 511 stores the 1-bit information which shows the state of a lock/unlocking. The lock key freeze information 512 stores the 1-bit information which shows a lock key freeze / lock key freeze release. A lock key 513 is information managed as a key given to the IC chip 104 concerned.

[0035] Drawing 6 is drawing explaining the state transition of the lock information 511 recorded on the IC chip 104, and the lock key freeze information 512. The state of the lock information 511 and the lock key freeze information 512 has three, the state 601 of a lock and a lock key freeze, the state 602 of unlocking and a lock key freeze, and the state 603 of unlocking and lock key freeze release.

[0036] A state 601 is in the state which cannot use the securities 103 concerned and cannot update a lock key 513. It can change in the state 602 from a state 601 by using the right lock key.

[0037] A state 602 can use the securities 103 concerned, and is in the state which cannot update a lock key 513. It can change in the state 603 from a state 602 by using the right lock key. Moreover, it can change in the state 601 from a state 602 by using the right lock key.

[0038] A state 603 can use the securities 103 concerned, and is in the state which can update a lock key 513. It can change in the state 602 from a state 603 by using the right lock key.

[0039] Drawing 7 A and drawing 7 B are flow charts which show the flow of processing of the lock / lock key processing section 310 of the management server 101. A lock / lock key processing section 310 receives the demand inputted from the keyboard etc. about the target securities 103 (Step 701). a demand is shown below -- there are four kinds (1) Change into a lock state the lock information 511 on the IC chip 104 carried in the securities 103 concerned from an unlocking state. (2) Change the lock information 511 into an unlocking state from a lock state. Whether the lock key freeze information 512 is changed into a lock key freeze state or it changes into the state of lock key freeze release need to be specified of this demand. (3) Update a lock key 513 after changing an unlocking state and the lock key freeze information 512 into a lock key freeze release state for the lock information 511. (4) Change a lock state and the lock key freeze information 512 into a lock key freeze state for the lock information 511 after updating a lock key 513.

[0040] Next, a lock / lock key processing section 310 judges whether the lock key registered into the lock key or the lock key managed table 308 which is the lock key which received the notice from old management origin, and was inputted from the keyboard 304 etc., and the lock key 513 on the IC chip 104 are in agreement in whether a lock key 513 is right (Step 702). Since the lock key 513 is not updated yet here, it will collate about the lock key before renewal of a lock key, and the lock key is either of the lock keys which received the notice from the lock key which the management server 101 concerned manages, or other management places of business. If a lock key 513 is not right (Step 702, error), it considers as a processing end.

[0041] If a lock key 513 is right, unlocking processing which changes the lock information 511 on the IC chip 104 concerned into an unlocking state will be performed (Step 703). Next, if renewal of a lock key is not demanded (Step 704), it goes to Step 709. When renewal of a lock key is demanded, it judges whether a lock key 513 is right (Step 705). Here, the check of Step 702 will be repeated and it is judged with a lock key 513 being right. Next, the lock key freeze information 512 is read, and if it is in a lock

key freeze state (Step 706, freeze), this will be changed into the state of lock key freeze release (Step 707). Next, with reference to the lock key managed table 308, the lock key 513 on the IC chip 104 is updated to the new lock key under management of the management server 101 (Step 708).
[0042] Next, it moves to drawing 7 B and judges whether a lock / lock key processing section 310 freezes a lock key (Step 709). When specification of a lock key freeze is carried out by a demand (1), (4), and (2), the freeze of a lock key is required. In not carrying out a lock key freeze, it goes to Step 712. Next, it judges whether a lock key 513 is right (Step 710). When renewal of a lock key of Step 708 is carried out, coincidence with the lock key on the lock key managed table 308 and the lock key 513 after updating is judged, and it is judged with naturally a lock key 513 being right. When renewal of a lock key of Step 708 has not been carried out, the check of Step 702 will be repeated and it is judged with a lock key 513 being right. if a lock key is right (Step 710 -- right), the lock key freeze information 512 will be changed into a lock key freeze state (Step 711)
[0043] Next, it judges whether a lock / lock key processing section 310 changes the lock information 511 into a lock state (Step 712). It is necessary to change the lock information 511 into a lock state about a demand (1) and (4). In locking (Step 712), it judges whether a lock key 513 is right again (Step 713). The check of Step 702 and Step 710 will be repeated at a demand (1) and the case of (4), and it is judged with a lock key 513 being right. if a lock key is right (Step 713 -- right), the lock key freeze information 512 is in the state of a freeze (Step 714, freeze), and when the lock information 511 is in an unlocking state, (Step 715, unlocking), and lock processing that changes the lock information 511 into a lock state will be performed (Step 716)
[0044] When the lock key freeze information 512 which is contradictory to the judgment of Step 709 at Step 714 when there is an error of a lock key at Step 710, it does not lock at Step 712 and there is an error of a lock key at Step 713 is in a lock key freeze release state, and when the lock information 511 is in a lock state at Step 715, it considers as a processing end immediately.
[0045] Although the check with a right lock key 513 was based on the judgment with the lock key which suited under another management or the lock key on the lock key managed table 308, and the lock key 513 in agreement on the IC chip 104 with the above-mentioned operation form If a lock key with a plaintext is transmitted to the IC chip 104 or a lock key with a plaintext is transmitted to it from the IC chip 104 through IC chip reading and write-in equipment 307 to the management server 101 from the management server 101, the danger that security will be broken will become high. For example, if the electromagnetic wave sent out from IC chip reading and write-in equipment 307 is intercepted, the lock key transmitted between the management server 101 and the IC chip 104 can be known. In order to avoid such risk, it is desirable to transmit the numeric value which made the lock key the cryptographic key, without transmitting a direct lock key, and was enciphered by the lock key. For example, the random number which enciphered the random number which used as the public key the lock key registered into the lock key managed table 308, and a lock / lock key processing section 310 made generate a random number, and was generated with this public key, and was enciphered, and the original random number are transmitted to the IC chip 104. The lock key right-or-wrong judging program 522 of the IC chip 104 When the command of a lock key right-or-wrong judging is received, the random number with which the code decode program 521 was enciphered by the lock key 513 saved as a private key is decoded. It is able for the lock key right-or-wrong judging program 522 to compare with the original random number the random number by which decode was carried out, to judge the right or wrong of a lock key, and to notify the result (positive or no) to the lock / lock key processing section 310 of the management server 101. In this case, the lock key which suited under another management or the lock key on the lock key managed table 308, and the lock key 513 on the IC chip 104 have the correspondence relation of a public key pair, and, generally the same value does not become. Therefore, the lock key which can generally creep and is under that management, and the lock key 513 on the IC chip 104 do not need to be the same values, and should just be the numeric value which had a predetermined correspondence relation.
[0046] finishing [the renewal program 523 of lock state reference on the IC chip 104 / a judgment of the right or wrong of a lock key] when the command which requires reference of the lock information 511

is received from the management server 101 or the operating server 105 -- it is -- it is not involved nothing but transmits to content of lock information 511 demand-origin However, this demand will not be answered if it is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires renewal of the lock information 511 is received. Moreover, if the renewal program 523 of lock state reference is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires the reference or updating of the lock key freeze information 512 is received, it will not answer this demand.
[0047] Similarly, if the renewal program 524 of a lock key on the IC chip 104 is not after judging if a lock key is right by the lock key right-or-wrong judging program 522, when the command which requires renewal of a lock key 513 is received, it will not answer this demand. In using a public key pair as a lock key, after transmitting the updating demand command of a lock key 513 to the IC chip 104 and obtaining a response, a lock / lock key processing section 310 enciphers the lock key after updating (private key) by the old lock key (public key), and transmits to the IC chip 104. The renewal program 524 of a lock key is decoded by the old lock key (private key) in which the encryption information received through the code decode program 521 is stored by the lock key 513, and transposes a lock key 513 to the new lock key (private key) by which decode was carried out. In using a common key instead of a public key pair as a lock key, a lock / lock key processing section 310 enciphers a new lock key (common key) by the old lock key (common key) similarly, it transmits to the IC chip 104, the encryption information which the renewal program 524 of a lock key received is decoded by the old lock key (common key), and it transposes to the lock key which was able to obtain the lock key 513.
[0048] The lock key right-or-wrong judging program 522 has a lock key right-or-wrong judging flag on storage 505, and saves the result (positive or no) of a right-or-wrong judging of a lock key. And this lock key right-or-wrong judging flag is reset to an initial state (no) at the time of each processing end of processing (unlocking processing) of Step 703, processing (renewal of a lock key) of Step 708, processing (freezing treatment of a lock key) of Step 711, and processing (lock processing) of Step 716. In any [of demand (1) - (4)] case, this flag is reset by the state of no by such composition at the time of a processing end.
[0049] In addition, although the lock key freeze information 512 was formed in the IC chip 104, and updating of a lock key 513 was enabled with the above-mentioned operation gestalt only when the lock key freeze information 512 was in a lock key freeze release state, the lock key freeze information 512 is not established, but when a lock key is right irrespective of the state of the lock information 511, this invention can be carried out also in the form which degenerated so that lock key 513 updating might always be enabled. In this case, a demand becomes three kinds of (1) and (2), (3), or (4), and processing of Steps 706, 707,709,710,711, and 714 is excepted.
[0050] Moreover, an identification number (ID) like the serial number of the IC chip 104 concerned may be given to the storage 505 of the IC chip 104, the correspondence table of this ID and lock key may be prepared in the lock key managed table 308, and the securities 103 which carried the IC chip 104 by the pair of ID and a lock key may be managed. Moreover, if it is used in order to only call the IC chip 104 theft prevention under storage or transportation, the management server 101 is able to give and manage the same lock key for the IC chip 104 of all the securities 103 put under management. Only as for the management server 101 concerned, the securities 103 which carry the IC chip 104 set in the lock state recovered from the theft etc. change into the state of unlocking.
[0051] Or if the value which shows the invalid of the lock key 513 beforehand specified specially to the lock information 511 on the IC chip 104 as a modification about the above-mentioned operation gestalt is set up and it will be made the structure which cannot return to an unlocking state eternally, electronic abandonment processing can be given to the securities of this invention the same with carrying out decision (abandonment) processing so that the reuse of the gift certificate after use cannot be carried out, for example etc.
[0052] What is necessary is just to opt for the function of the program which is the balance of the required grade of security, and the cost of the IC chip 104, and stores in the hardware of the IC chip 104, and the IC chip 104, and the IC chip 104 performs since various deformation can be performed in

operation of this invention like described above.
[0053] It is possible to judge from the information on IC chip carried in the securities concerned, to perform operating processing justly or to prevent unjust use as mentioned above, without an operating server asking a management server the propriety of the execution of operating processing to the securities concerned by the online network etc. with this operation gestalt. Moreover, the method of this invention is applied, and the reuse can be enabled when the once squeezed securities which cannot be used are able to be regained under management of a just management server.
[0054] Since the propriety of use of the securities concerned can be judged using the information on IC chip carried in securities according to this operation gestalt as explained above, it is possible to discriminate on that spot whether they are the securities squeezed unjustly, and to prevent unjust use.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the outline composition of an operation gestalt.
[Drawing 2] It is drawing explaining the use procedure of the securities which carry IC chip of an operation gestalt.
[Drawing 3] It is drawing showing the outline composition of the management server 101 of an operation gestalt.
[Drawing 4] It is drawing showing the outline composition of the operating server 105 of an operation gestalt.
[Drawing 5] It is drawing showing the internal configuration of the IC chip 104 carried in the securities 103 of an operation gestalt.
[Drawing 6] It is drawing showing the state transition of the lock information 511 on an operation gestalt, and the lock key freeze information 512.
[Drawing 7 A] It is the flow chart which shows the procedure of the lock / lock key processing section 310 of the management server 101 of an operation gestalt.
[Drawing 7 B] It is the flow chart (continuation) which shows the procedure of the lock / lock key processing section 310 of the management server 101 of an operation gestalt.
[Description of Notations]
101 [-- IC chip, 105 / -- An operating server, 308 / -- A lock key managed table, 310 / -- A lock / lock key processing section, 511 / -- Lock information, 512 / -- Lock key freeze information, 513 / -- Lock key] -- A management server, 103 -- Securities, 104

[Translation done.]

* NOTICES *

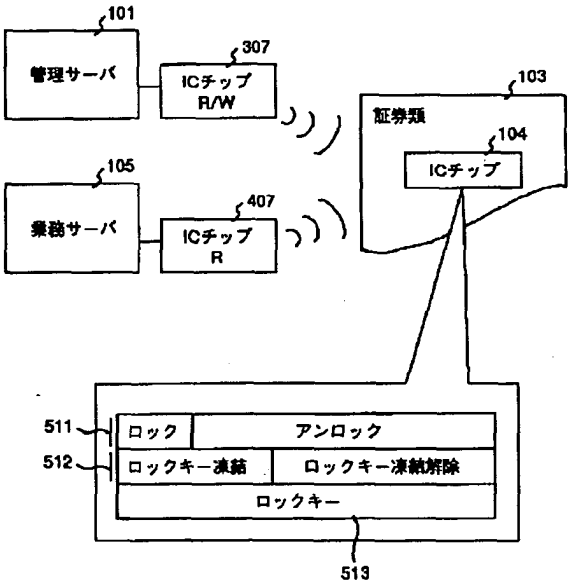
Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

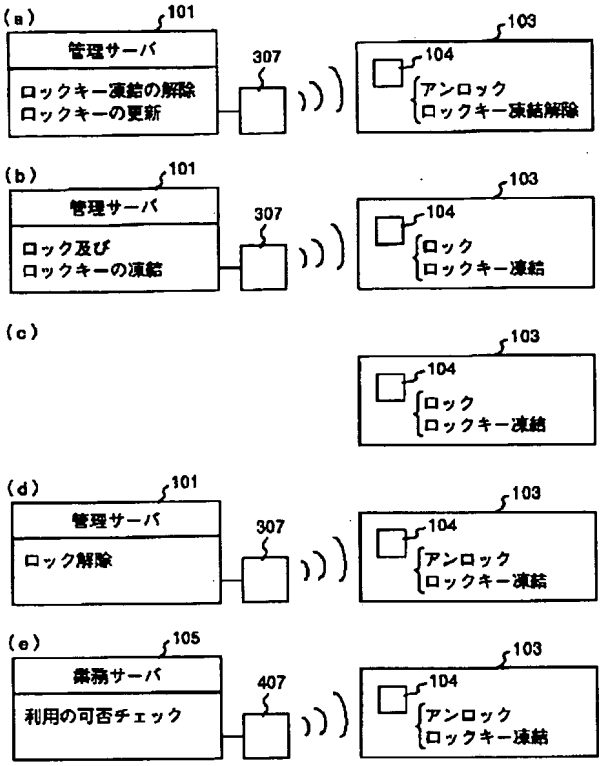
[Drawing 1]

図 1

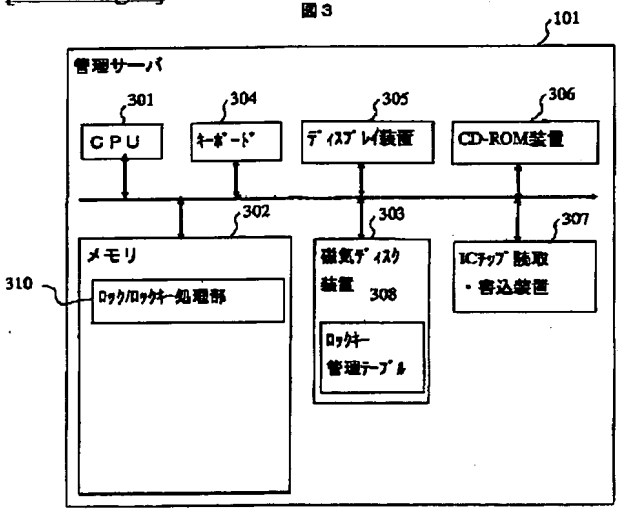


[Drawing 2]

図 2

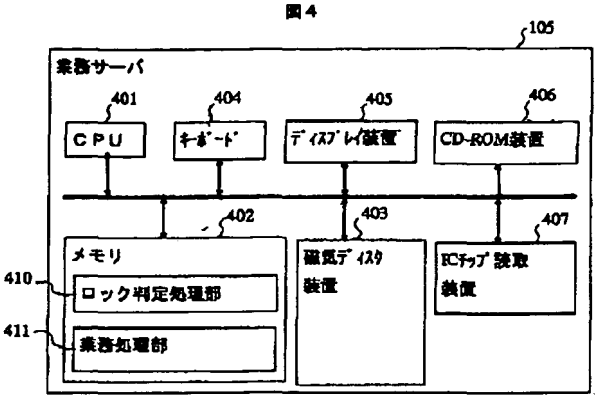


[Drawing 3]



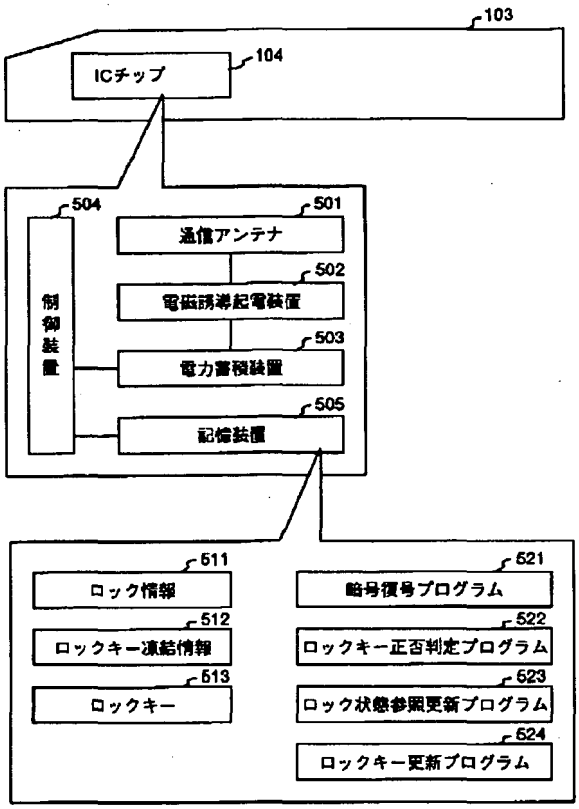
[Drawing 4]

図4



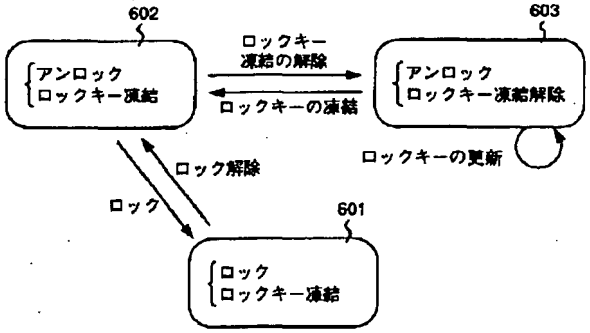
[Drawing 5]

図 5



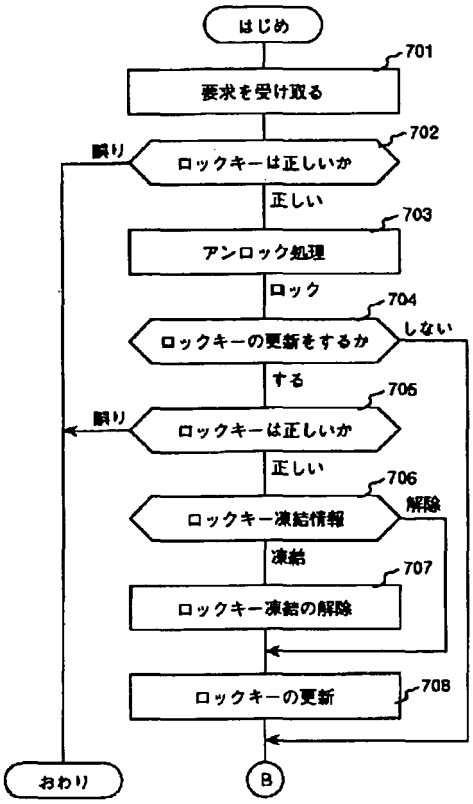
[Drawing 6]

図 6



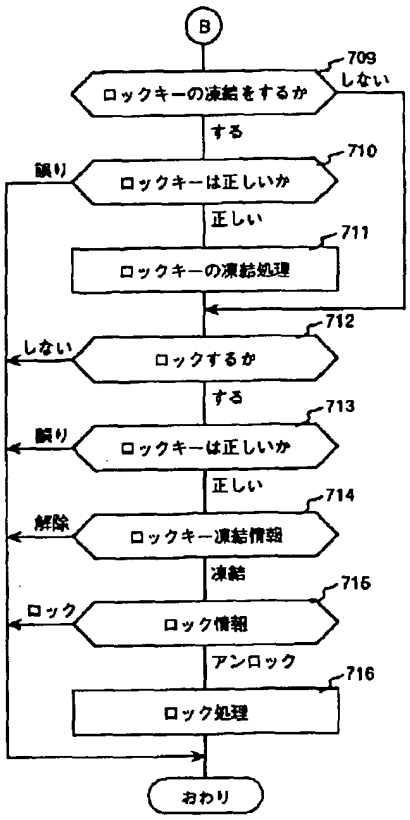
[Drawing 7 A]

図 7 A



[Drawing 7 B]

図 7B



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－260580
（P2001－260580A）
(43)公開日　平成13年９月25日(2001.9.25)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｂ４２Ｄ　15/10	５３１	Ｂ４２Ｄ　15/10	５３１Ｂ　２Ｃ００５
	５２１		５２１　３Ｅ０４１
Ｇ０６Ｆ　17/60	２１４	Ｇ０６Ｆ　17/60	２１４　５Ｂ０３５
	５１０		５１０　５Ｂ０４９
	５１２		５１２　５Ｂ０５５

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願2000－77750(P2000－77750)

(22)出願日　平成12年３月15日(2000.3.15)

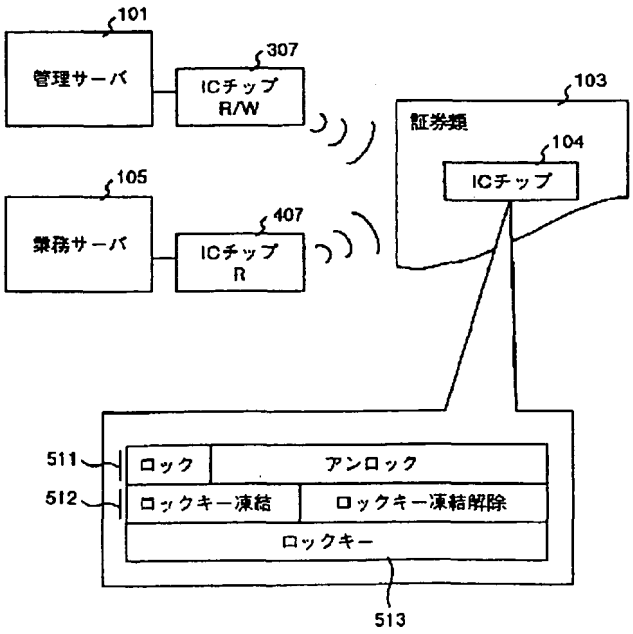
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　戸田　幸利
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所サービス事業部内
(74)代理人　100068504
弁理士　小川　勝男　（外１名）

最終頁に続く

(54)【発明の名称】　ＩＣチップを搭載する紙幣及び有価証券類並びにその不正利用防止方法

(57)【要約】
【課題】　証券類が搾取されたことを識別して不正利用を防ぐとともに、正規な管理元に取り戻せた場合には再利用が可能な証券類及びその不正利用防止方法を提供する。
【解決手段】　紙幣、株券など有価な証券類１０３に微細なＩＣチップ１０４が搭載されており、ＩＣチップ１０４の記憶装置はロック情報５１１及びロックキーを格納する。ロック情報５１１はロック／アンロックいずれかの状態を保持する。業務サーバ１０５は、ＩＣチップ読取装置４０７を介してロック情報５１１の状態を読み取り、それがアンロック状態でなければ業務処理を開始しない。管理サーバ１０１は、ＩＣチップ読取・書込装置３０７を介してＩＣチップ１０４と通信し、ロックキー５１３が正しいものと認証した後に、必要に応じてロック情報５１１の状態を変更する。

図　1



【特許請求の範囲】

【請求項1】非接触で読み書き可能なICチップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記ICチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能な情報と、外部からの要求に応答して前記情報を変更する前記ICチップ内で実行可能なプログラムとを格納する記憶装置を有することを特徴とするICチップを搭載する有価証券類。

【請求項2】非接触で読み書き可能なICチップを搭載する紙幣、商品券、株券、債券など有価の証券類の不正利用防止方法であって、前記ICチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック/アンロック情報と、外部からの要求に応答して前記ロック/アンロック情報の参照と更新を行う前記ICチップ内で実行可能なプログラムとを格納する記憶装置を有し、前記証券類の利用を禁止するように外部の計算機によって前記ICチップに前記ロック/アンロック情報をロック状態に設定するように指令し、前記証券類を利用可能とするように外部の計算機によって前記ICチップに前記ロック/アンロック情報をアンロック状態に設定するように指令し、外部の計算機によって前記ICチップ上の前記ロック/アンロック情報を参照し、前記ロック/アンロック情報がアンロック状態の場合に業務処理を開始することを特徴とするICチップを搭載する有価証券類の不正利用防止方法。

【請求項3】前記ロック/アンロック情報を更新する前記外部の計算機は、その記憶装置に第1のキー情報を保存し、前記ICチップはその記憶装置に第1のキー情報と対になる第2のキー情報を保存し、前記ロック/アンロック情報を更新する前記外部の計算機と前記ICチップとの間で第1のキー情報と第2のキー情報とが所定の対応関係をもつことを認証したとき、前記ICチップによって前記ロック/アンロック情報の更新を行うことを特徴とする請求項2記載のICチップを搭載する有価証券類の不正利用防止方法。

【請求項4】非接触で読み書き可能なICチップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記ICチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック/アンロック情報と、外部からの要求に応答して前記ロック/アンロック情報の参照と更新を行う前記ICチップ内で実行可能なプログラムとを格納する記憶装置を有するところの有価証券類と、前記ICチップに対して前記ロック/アンロック情報を更新するよう指令する管理用計算機と、前記ICチップに要求して前記ロック/アンロック情報を参照し、前記ロック/アンロック情報がアンロック状態の場合に業務処理を開始する業務処理用計算機とを有することを特徴とするICチップを搭載する有価証券類の不正利用防止システム。

【請求項5】前記ロック/アンロック情報を更新する前記管理用計算機は、その記憶装置に第1のキー情報を保存し、前記ICチップはその記憶装置に第1のキー情報と対になる第2のキー情報を保存し、前記ロック/アンロック情報を更新する前記管理用計算機と前記ICチップとの間で第1のキー情報と第2のキー情報とが所定の対応関係をもつことを認証したとき、前記ICチップが前記ロック/アンロック情報の更新を行うことを特徴とする請求項4記載のICチップを搭載する有価証券類の不正利用防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、金融/サービス/運送業などの取扱い対象となる証券類及びその不正利用防止方法に係わり、特に紙幣、商品券、株券、債券、手形、小切手など何らかの価値を持つ有価証券類（以下、単に証券類と呼ぶ）を保管、運搬する際に盗難等で不正に取得した証券類を使用不可の状態にしたり、正規に入手した証券類の有効性を証明する不正利用防止システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】従来、取引の支払いをしたり、商品の引換えをしたり、株式会社に出資したり、第三者から事業資金を得たり、代金の支払いの約束をしたり、金銭の支払いの約束をしたりと、様々な価値をもつ権利を表す証券類が世の中に流通している。

【0003】これらの証券類を一時的に保管したり、運搬したりする場合には、物理的な鍵のかかる金庫やトランクなどに鍵を掛けたり、盗難を防ぐために警備員を配置したりするが、証券類には特に何らかの加工を加えることはせず、現状はそのまま利用可能な状態にある。

【0004】なお、近年は街頭に置かれた無人のATM/CD端末を、パワーシャベルなどといった重機を使って破壊し、保管してある現金を搾取したりすることがあるので、ATM/CD端末に破壊などの不正行為を働いた場合に、紙幣にインクを吹き付けたりして盗難にあった事実を記したりする技術がある。

【0005】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。すなわち一旦盗難にあった証券類は、正規に利用されるものと区別のつかない状態にあって不正に利用されたり、インクなどの目印が付いてしまい、正当な所有者が取り戻すことができても再利用できないという問題がある。またインクが搾取される証券類の全数に確実につかない可能性もある。

【0006】本発明の目的は上記問題を解決し、盗難された証券類の不正利用を防止したり、正規の管理元に取り戻した場合に再利用することが可能な証券類及びその不正利用防止方法を提供することにある。

【0007】

【課題を解決するための手段】本発明は、保管または輸

送される証券類について、証券類に搭載したＩＣチップの情報を読んで、不正に搾取されたものとして利用してはならないか、あるいは正規に譲渡されたものとして利用して良いものかどうかを識別可能にするものである。

【０００８】本発明において、証券類の利用の可否を識別するには、証券類に搭載したＩＣチップに利用可否の識別情報を登録することによって行う。近年になってサイズが数ミリ（２～３㎜）角の非接触通信式のＩＣチップ（ＲＦＩＤ）の開発が新聞等で発表されてきている。こういった微細なＩＣチップ製造技術がさらに進めば、紙幣や有価証券などに装着できるようなＩＣチップが登場する。本発明では、こういった紙などの薄い媒体に微細なＩＣチップを本発明でいう証券類の一枚ずつに搭載し、当該証券類各々の有効性の情報をもたせ、それらの情報を読み込んで識別することを可能にするものである。

【０００９】証券類に搭載するＩＣチップへの読み書きは、当該証券類を保管／運搬の管理をする法人または事業所の管理単位に可能であり、ＩＣチップへの情報の書き込みに関するセキュリティも管理する。よって正規の管理元が保管または運搬する証券類を他者が搾取したとき、当該証券類に搭載するＩＣチップの情報が利用不可の状態であることを示すようにしておき、証券類の利用時にこの情報を読み出すことによって、当該証券類が不正に搾取されたものであることを識別でき、これらをこの状態で利用することを拒否することによって、不正利用を防止することが可能になる。証券類に搭載するＩＣチップの情報の読み取りは、証券類を業務処理に使用する際にＩＣチップ読取装置で読み取ることができるようにしておく。

【００１０】一方、証券類に搭載したＩＣチップへの情報の書き込みは、セキュリティのための制御情報（暗証番号、暗号鍵など）により、このような制御情報を保持する管理用計算機のみが行えるようにし、制御情報を知らない第三者がＩＣチップの情報を書き換えることはできないようにする。

【００１１】またある管理元が管理する証券類を別の管理元に正規に移管する場合には、新しい管理元が譲渡対象となる証券類に搭載するＩＣチップの情報を書き換えるために必要な独自の制御情報に変更できるように、古い管理元が設定していた制御情報を用いて制御情報の書き換え制限を解除することにより、新しい管理元が管理する制御情報に変更することができる。こうして新たな管理元は、自分の管理下のセキュリティ制御情報を用いて証券類に搭載するＩＣチップの情報を必要に応じて書き換えることができるようになる。

【００１２】よって一旦不正に搾取された証券類でも、元のＩＣチップの情報を書き換えできる正当なセキュリティ制御情報をもつ管理元に戻せれば、利用不可状態となっていた証券類のＩＣチップの情報を利用可能な状態に戻すことができ、問題なく再利用することができるようになる。

【００１３】以上のように本発明の証券類及びその不正利用防止方法によれば、非接触の通信によりＩＣチップを搭載した管理単位全数について確実に証券類の利用可否の情報を読み書きできるので、搾取された証券類を識別でき、その不正利用を防ぐことができ、さらに正規の所有者の手に戻れば再度利用可能な状態に戻すことも可能である。

【００１４】

【発明の実施の形態】以下に証券類の不正利用防止を可能とする実施形態について図面を用いて説明する。

【００１５】図１は、本実施形態の概略構成を示す図である。証券類１０３には微細なＩＣチップ１０４が装着されている。ＩＣチップ１０４は、証券類１０３を構成する２枚の紙の間にすき込むか、あるいはＩＣチップ１０４を封入したシールを証券類１０３に接着するなどの方法によって証券類１０３に装着されている。いずれにしてもＩＣチップ１０４は、証券類１０３を使用不可能にするほど破損することなく、そのＩＣチップ１０４を証券類１０３から引き離すことができないような方法で証券類１０３に装着されている。ＩＣチップ１０４内の記憶装置にはロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３を記録する。ロック情報５１１は、ロック状態とアンロック状態のいずれかの状態をもつ。ロック状態は業務処理のために証券類１０３を利用できない状態であり、アンロック状態は業務処理のために証券類１０３を利用できる状態である。ロックキー５１３は、ロック情報５１１、ロックキー凍結情報５１２およびロックキー５１３自体を変更するために必要な鍵（パスワード、暗号鍵など）となるビット列である。ロックキー凍結情報５１２は、ロックキー凍結状態とロックキー凍結解除状態のいずれかの状態をもつ。ロックキー凍結状態はロックキー５１３を凍結し更新できない状態であり、ロックキー凍結解除状態はロックキー５１３を更新できる状態である。

【００１６】管理サーバ１０１は、ロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３を更新する権限をもち、ロックキー５１３を管理する計算機であり、ＩＣチップ読取・書込装置３０７を接続する。管理サーバ１０１は、ＩＣチップ読取・書込装置３０７を介して証券類１０３に搭載されたＩＣチップ１０４上の情報を非接触で読み取り、ロック情報５１１の変更、ロックキー凍結情報５１２の変更及びロックキー５１３の更新を行う。

【００１７】業務サーバ１０５は、証券類１０３に関する業務処理を行う計算機であり、ＩＣチップ読取装置４０７を接続する。業務サーバ１０５は、ＩＣチップ読取装置４０７を介して証券類１０３のＩＣチップ１０４上のロック情報５１１にアクセスし、ロック情報５１１が

アンロック状態であれば証券類１０３を取り扱う業務処理を行い、ロック状態であれば業務処理を行わない。

【００１８】図２は、ＩＣチップ１０４の装着された証券類１０３を利用する手順の例を説明する図である。ＩＣチップ１０４の装着された証券類１０３は、証券類１０３の製造過程から入ってきた証券類１０３であり最初に利用されるものであるか、または他の管理サーバによって管理されていたものであって最初に当該管理サーバ１０１の管理下に入るものとし、ロック情報５１１がロック状態、ロックキー凍結情報５１２がロックキー凍結の状態にあるものとする。

【００１９】図２（ａ）は、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロックキー凍結情報５１２をロックキー凍結解除し、ロックキー５１３を自分の管理するロックキーに更新するステップである。図２（ｂ）は、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロック情報５１１をロック状態にし、ロックキー凍結情報５１２をロックキー凍結の状態に変更するステップである。図２（ｃ）は、この状態の証券類１０３を保管または運搬するステップを示す。この状態の証券類１０３を業務処理に利用することはできない。また他の管理サーバによって不当にロックキー５１３を自分の管理下のロックキーに更新することはできない。

【００２０】図２（ｄ）は、この証券類１０３を業務処理に利用するために、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロック情報５１１をアンロックの状態に変更するステップである。図２（ｅ）では、業務サーバ１０５が証券類１０３上のＩＣチップ１０４のロック情報５１１にアクセスして利用の可否をチェックする。ロック情報５１１がアンロック状態であればこの証券類１０３に関する業務処理を開始し、ロック情報５１１がロック状態であればこの証券類１０３についての業務処理を行わない。従って保管または運搬中に盗難等に会った証券類１０３は業務処理されない。

【００２１】上記の証券類１０３がある管理サーバの管理下から別の管理サーバの管理下に移るとは、例えば証券類１０３がある金融機関から別の金融機関に譲渡されたり、事業所間で譲渡される場合を想定している。従ってセキュリティの問題が生じないのであれば、ＩＣチップ１０４のロック情報５１１がアンロック、ロックキー凍結情報５１２がロックキー凍結解除の状態で証券類１０３を事業所間で譲渡しても構わない。

【００２２】図３は、管理サーバ１０１の概略構成を示す図である。図３に示すように管理サーバ１０１は、ＣＰＵ３０１と、メモリ３０２と、磁気ディスク装置３０３と、キーボード装置３０４と、ディスプレイ装置３０５と、ＣＤ－ＲＯＭ装置３０６と、ＩＣチップ読取・書込装置３０７を有している。磁気ディスク装置３０３はロックキー管理テーブル３０８を格納している。管理サーバ１０１の全体が携帯情報処理装置であってもよい。

【００２３】ＣＰＵ３０１は、管理サーバ１０１全体の動作を制御する装置である。メモリ３０２は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置３０３は、各種処理プログラムやデータを格納しておく記憶装置である。キーボード装置３０４は、データ入力のための装置であり、ディスプレイ装置３０５は各種データの表示を行う装置である。ＣＤ－ＲＯＭ装置３０６は、各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。ＩＣチップ読取・書込装置３０７は、証券類１０３に搭載するＩＣチップ１０４との間で非接触で情報の読み書きをする装置である。

【００２４】ロックキー管理テーブル３０８は、当該管理サーバ１０１が管理するロックキーを格納するテーブルである。

【００２５】ロック／ロックキー処理部３１０は、メモリ３０２に格納され、図２に示すように証券類１０３のＩＣチップ１０４に記録されたロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３の管理に係わる処理を行うプログラムであり、ＣＰＵ３０１によって実行される。

【００２６】ＣＤ－ＲＯＭ等の記録媒体に記録されたロック／ロックキー処理部３１０を磁気ディスク装置３０３等に格納した後、メモリ３０２にロードして実行するものとする。なおこのプログラムを記録する記録媒体としてＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００２７】図４は、業務サーバ１０５の概略構成を示す図である。図４に示すように業務サーバ１０５は、ＣＰＵ４０１と、メモリ４０２と、磁気ディスク装置４０３と、キーボード装置４０４と、ディスプレイ装置４０５と、ＣＤ－ＲＯＭ装置４０６と、ＩＣチップ読取装置４０７とを有している。

【００２８】ＣＰＵ４０１は、業務サーバ１０５全体の動作を制御する装置である。メモリ４０２は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置４０３は、各種処理プログラムやデータを格納しておく記憶装置である。ＩＣチップ読取装置４０７は、証券類１０３に搭載するＩＣチップ１０４から非接触でロック情報５１１を読み取る装置である。

【００２９】メモリ４０２は、ロック判定処理部４１０及び業務処理部４１１を格納する。ロック判定処理部４１０は、証券類１０３に搭載するＩＣチップ１０４のロック情報５１１を読み込み、当該証券類１０３の利用の可否を判定する処理を行うプログラムである。業務処理部４１１は、利用可能と判定した証券類１０３に関する業務アプリケーションの処理を行う処理部である。

【００３０】ＣＤ－ＲＯＭ等の記録媒体に記録されたロック判定処理部４１０を含むプログラムを磁気ディスク装置４０３等に格納した後、メモリにロードして実行す

るものとする。なおこのプログラムを記録する記録媒体としてCD-ROM以外の他の記録媒体でも良い。

【0031】図5は、証券類103に搭載されるICチップ104の内部構成を示す図である。ICチップ104は、微細な半導体チップであり、図5に示すように通信アンテナ501、電磁誘導起電装置502、電力蓄積装置503、制御装置504及び記憶装置505を有している。

【0032】通信アンテナ501は、ICチップ104とICチップ読取・書込装置307又はICチップ読取装置407との間で情報を送受信したり、ICチップ104を駆動する電源となる電力供給のための電磁波をICチップ読取・書込装置307又はICチップ読取装置407から受けたりする装置である。電磁誘導起電装置502は、通信アンテナ501で受けた電磁波を電磁誘導により電力に変換する装置である。電力蓄積装置503は、電磁誘導起電装置502で起電した電力を蓄積して、ICチップ104を駆動するための電源とする装置である。

【0033】制御装置504は、マイクロプロセッサを含み、ICチップ104全体の動作を制御する装置である。記憶装置505は、ロック情報511、ロックキー凍結情報512及びロックキー513の管理情報と、暗号復号プログラム521、ロックキー正否判定プログラム522、ロック状態参照更新プログラム523、ロックキー更新プログラム524など各種プログラムを格納する。

【0034】ロック情報511は、ロック／アンロックの状態を示す1ビットの情報を格納する。ロックキー凍結情報512は、ロックキー凍結／ロックキー凍結解除を示す1ビットの情報を格納する。ロックキー513は当該ICチップ104に付与される鍵として管理される情報である。

【0035】図6は、ICチップ104に記録されるロック情報511及びロックキー凍結情報512の状態遷移について説明する図である。ロック情報511及びロックキー凍結情報512の状態は、ロックかつロックキー凍結の状態601と、アンロックかつロックキー凍結の状態602と、アンロックかつロックキー凍結解除の状態603の3つがある。

【0036】状態601は、当該証券類103を利用不可能で、かつロックキー513を更新することができない状態である。正しいロックキーを用いることによって状態601から状態602に遷移することができる。

【0037】状態602は、当該証券類103を利用することが可能で、かつロックキー513を更新することができない状態である。正しいロックキーを用いることによって状態602から状態603に遷移することができる。また正しいロックキーを用いることによって状態602から状態601に遷移することができる。

【0038】状態603は、当該証券類103を利用することが可能で、かつロックキー513を更新することができる状態である。正しいロックキーを用いることによって状態603から状態602に遷移することができる。

【0039】図7A及び図7Bは、管理サーバ101のロック／ロックキー処理部310の処理の流れを示すフローチャートである。ロック／ロックキー処理部310は、対象とする証券類103についてキーボード等から入力された要求を受け取る（ステップ701）。要求は次に示す4種類ある。（1）当該証券類103に搭載されたICチップ104のロック情報511をアンロック状態からロック状態に変更する。（2）ロック情報511をロック状態からアンロック状態に変更する。この要求ではロックキー凍結情報512をロックキー凍結状態にするか、ロックキー凍結解除の状態にするかの指定が必要である。（3）ロック情報511をアンロック状態、ロックキー凍結情報512をロックキー凍結解除状態にした後にロックキー513を更新する。（4）ロックキー513を更新した後にロック情報511をロック状態、ロックキー凍結情報512をロックキー凍結状態にする。

【0040】次にロック／ロックキー処理部310は、ロックキー513が正しいか否か、例えば古い管理元から通知を受けたロックキーであってキーボード304などから入力されたロックキー又はロックキー管理テーブル308に登録されているロックキーとICチップ104上のロックキー513とが一致するか否か判定する（ステップ702）。ここではまだロックキー513が更新されていないため、ロックキー更新前のロックキーについて照合することになり、そのロックキーは当該管理サーバ101が管理するロックキー又は他の管理事業所から通知を受けたロックキーのいずれかである。ロックキー513が正しくなければ（ステップ702，誤り）、処理終了とする。

【0041】ロックキー513が正しければ、当該ICチップ104上のロック情報511をアンロック状態に変更するアンロック処理を行う（ステップ703）。次にロックキーの更新が要求されていなければ（ステップ704，しない）、ステップ709へ行く。ロックキーの更新が要求されている場合には、ロックキー513が正しいか否か判定する（ステップ705）。ここではステップ702のチェックが繰り返されることになり、ロックキー513が正しいと判定される。次にロックキー凍結情報512を読み取り、ロックキー凍結状態であれば（ステップ706，凍結）、これをロックキー凍結解除の状態にする（ステップ707）。次にロックキー管理テーブル308を参照してICチップ104上のロックキー513を管理サーバ101の管理下にある新しいロックキーに更新する（ステップ708）。

【0042】次に図7Bに移り、ロック／ロックキー処理部310は、ロックキーを凍結するか否か判定する（ステップ709）。要求（1）、（4）及び（2）でロックキー凍結の指定がされた場合にはロックキーの凍結が必要である。ロックキー凍結しない場合にはステップ712へ行く。次にロックキー513が正しいか否か判定する（ステップ710）。ステップ708のロックキー更新をした場合には、ロックキー管理テーブル308上のロックキーと更新後のロックキー513との一致が判定されるわけであり、当然ロックキー513が正しいと判定される。ステップ708のロックキー更新をしていない場合には、ステップ702のチェックが繰り返されることになり、ロックキー513が正しいと判定される。ロックキーが正しければ（ステップ710，正しい）、ロックキー凍結情報512をロックキー凍結状態にする（ステップ711）。

【0043】次にロック／ロックキー処理部310は、ロック情報511をロック状態にするか否か判定する（ステップ712）。要求（1）および（4）については、ロック情報511をロック状態にする必要がある。ロックする場合（ステップ712，する）には、再びロックキー513が正しいか否か判定する（ステップ713）。要求（1）及び（4）の場合にはステップ702及びステップ710のチェックが繰り返されることになり、ロックキー513が正しいと判定される。ロックキーが正しければ（ステップ713，正しい）、ロックキー凍結情報512が凍結の状態であり（ステップ714，凍結）、ロック情報511がアンロック状態の場合に（ステップ715，アンロック）、ロック情報511をロック状態に変更するロック処理を行う（ステップ716）。

【0044】ステップ710でロックキーの誤りがある場合、ステップ712でロックしない場合、ステップ713でロックキーの誤りがある場合、ステップ714でステップ709の判定と矛盾するロックキー凍結情報512がロックキー凍結解除状態の場合、およびステップ715でロック情報511がロック状態の場合には直ちに処理終了とする。

【0045】上記実施形態では、ロックキー513が正しいか否かのチェックは、別の管理下にあったロックキー又はロックキー管理テーブル308上のロックキーとICチップ104上のロックキー513とが一致するか否かの判定によっていたが、管理サーバ101からICチップ読取・書込装置307を介してICチップ104へ平文のままのロックキーを伝送したり、ICチップ104から管理サーバ101へ平文のままのロックキーを伝送すると、セキュリティが破られる危険性が高くなる。たとえばICチップ読取・書込装置307から送出される電磁波を盗聴すれば管理サーバ101とICチップ104との間に伝送されるロックキーを知り得ることになる。このような危険を避けるために、直接ロックキーを伝送せずにロックキーを暗号鍵とし、ロックキーによって暗号化した数値を伝送するのが望ましい。たとえばロックキー管理テーブル308に登録するロックキーを公開鍵とし、ロック／ロックキー処理部310が乱数を発生させ、発生した乱数をこの公開鍵で暗号化して暗号化した乱数と元の乱数とをICチップ104へ伝送する。ICチップ104のロックキー正否判定プログラム522は、ロックキー正否判定のコマンドを受けたとき、暗号復号プログラム521が秘密鍵として保存するロックキー513によって暗号化された乱数を復号し、ロックキー正否判定プログラム522が復号された乱数と元の乱数とを比較してロックキーの正否を判定し、その結果（正または否）を管理サーバ101のロック／ロックキー処理部310に通知することが可能である。この場合には別の管理下にあったロックキー又はロックキー管理テーブル308上のロックキーとICチップ104上のロックキー513とは公開鍵ペアの対応関係をもち、一般に同一値とはならない。従って一般にはいずれかの管理下にあるロックキーとICチップ104上のロックキー513とは同一値である必要はなく、所定の対応関係をもった数値であればよい。

【0046】ICチップ104上のロック状態参照更新プログラム523は、管理サーバ101又は業務サーバ105からそのロック情報511の参照を要求するコマンドを受けたとき、ロックキーの正否が判定済であるなしに係わらずロック情報511の内容を要求元に送信する。しかしロック情報511の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。またロック状態参照更新プログラム523は、ロックキー凍結情報512の参照又は更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。

【0047】同様にICチップ104上のロックキー更新プログラム524は、ロックキー513の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。ロックキーとして公開鍵ペアを使用する場合には、ロック／ロックキー処理部310は、ICチップ104へロックキー513の更新要求コマンドを伝送して応答を得た後に、更新後のロックキー（秘密鍵）を古いロックキー（公開鍵）で暗号化してICチップ104へ送信する。ロックキー更新プログラム524は、暗号復号プログラム521を介して受け取った暗号化情報をロックキー513に格納される古いロックキー（秘密鍵）で復号し、ロックキー513を復号された新しいロックキー（秘密鍵）に置き換える。ロックキーとして公開鍵ペアの代わりに共通鍵を

使用する場合には、同様にロック／ロックキー処理部３１０が新しいロックキー（共通鍵）を古いロックキー（共通鍵）で暗号化してＩＣチップ１０４へ送信し、ロックキー更新プログラム５２４が受け取った暗号化情報を古いロックキー（共通鍵）で復号し、ロックキー５１３を得られたロックキーに置き換える。

【００４８】ロックキー正否判定プログラム５２２は、記憶装置５０５上にロックキー正否判定フラグをもち、ロックキーの正否判定の結果（正または否）を保存する。そしてステップ７０３の処理（アンロック処理）、ステップ７０８の処理（ロックキーの更新）、ステップ７１１の処理（ロックキーの凍結処理）及びステップ７１６の処理（ロック処理）の各々の処理終了時にこのロックキー正否判定フラグを初期状態（否）にリセットする。このような構成によって要求（１）～（４）のいずれの場合にも処理終了時にこのフラグが否の状態にリセットされている。

【００４９】なお上記実施形態ではＩＣチップ１０４にロックキー凍結情報５１２を設け、ロックキー凍結情報５１２がロックキー凍結解除状態のときのみロックキー５１３を更新可能としたが、ロックキー凍結情報５１２を設けず、ロック情報５１１の状態に係わらずロックキーが正しい場合には常にロックキー５１３更新可能とするように縮退した形でも本発明を実施できる。その場合には要求は（１）及び（２）と（３）又は（４）の３種類となり、ステップ７０６，７０７，７０９，７１０，７１１及び７１４の処理は除外される。

【００５０】またＩＣチップ１０４の記憶装置５０５に当該ＩＣチップ１０４の製造番号のような識別番号（ＩＤ）をもたせ、ロックキー管理テーブル３０８にはこのＩＤとロックキーとの対応テーブルを設け、ＩＤとロックキーとの対でＩＣチップ１０４を搭載した証券類１０３を管理してもよい。またＩＣチップ１０４を単に保管又は輸送中の盗難防止という目的で使用するのであれば、管理サーバ１０１が管理下におくすべての証券類１０３のＩＣチップ１０４に同一のロックキーを付与して管理することも可能である。盗難等から取り戻されたロック状態におかれたＩＣチップ１０４を搭載する証券類１０３は、当該管理サーバ１０１のみがアンロックの状態にできる。

【００５１】あるいは上記実施形態についての変形例として、ＩＣチップ１０４のロック情報５１１に対し、あらかじめ特別に規定したロックキー５１３の無効を示す値を設定すると、永久にアンロック状態に戻れない仕組みにしておけば、例えば使用後の商品券を再使用できないように裁断（廃棄）処理するなどと同様に、本発明の証券類に対して、電子的な廃棄処理を施すことができる。

【００５２】以上述べたように、本発明の実施に当っては色々の変形ができるので、セキュリティの必要程度とＩＣチップ１０４のコストとの兼ね合いで、ＩＣチップ１０４のハードウェア及びＩＣチップ１０４に格納しＩＣチップ１０４が実行するプログラムの機能を決めればよい。

【００５３】上記のように本実施形態では、当該証券類に対する業務処理の実行の可否を業務サーバが管理サーバにオンラインネットワークなどで問い合わせることなく、当該証券類に搭載したＩＣチップの情報から判定し、正当に業務処理を行ったり、不正な利用を防止したりすることが可能である。また本発明の方法を適用し、一旦搾取された利用不可能な証券類を正当な管理サーバの管理下に取り戻せた場合は、その再利用を可能とすることができる。

【００５４】以上説明したように本実施形態によれば、証券類に搭載したＩＣチップの情報を用いて当該証券類の利用の可否を判定できるので、不正に搾取された証券類かどうかをその場で識別して不正利用を未然に防ぐことが可能である。

【００５５】

【発明の効果】本発明によれば、証券類に搭載したＩＣチップの情報を用いて不正に搾取された証券類を識別できるので、不正利用を防止することができ正当な管理元に戻せた場合に再利用可能な状態に戻すことが可能である。

【図面の簡単な説明】

【図１】実施形態の概略構成を示す図である。

【図２】実施形態のＩＣチップを搭載する証券類の利用手順を説明する図である。

【図３】実施形態の管理サーバ１０１の概略構成を示す図である。

【図４】実施形態の業務サーバ１０５の概略構成を示す図である。

【図５】実施形態の証券類１０３に搭載されるＩＣチップ１０４の内部構成を示す図である。

【図６】実施形態のロック情報５１１及びロックキー凍結情報５１２の状態遷移を示す図である。

【図７Ａ】実施形態の管理サーバ１０１のロック／ロックキー処理部３１０の処理手順を示すフローチャートである。

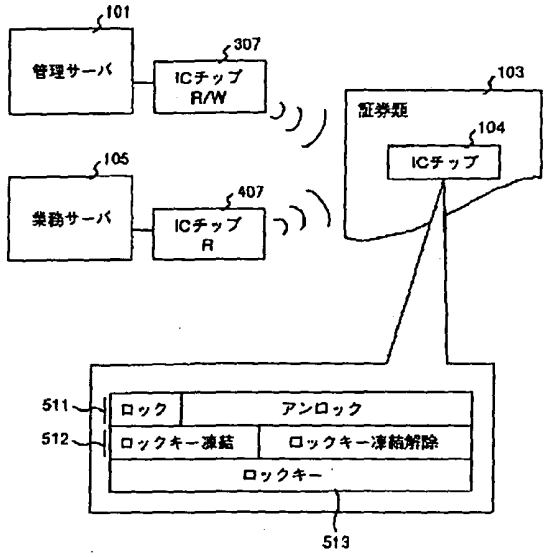
【図７Ｂ】実施形態の管理サーバ１０１のロック／ロックキー処理部３１０の処理手順を示すフローチャート（続き）である。

【符号の説明】

１０１…管理サーバ、１０３…証券類、１０４…ＩＣチップ、１０５…業務サーバ、３０８…ロックキー管理テーブル、３１０…ロック／ロックキー処理部、５１１…ロック情報、５１２…ロックキー凍結情報、５１３…ロックキー

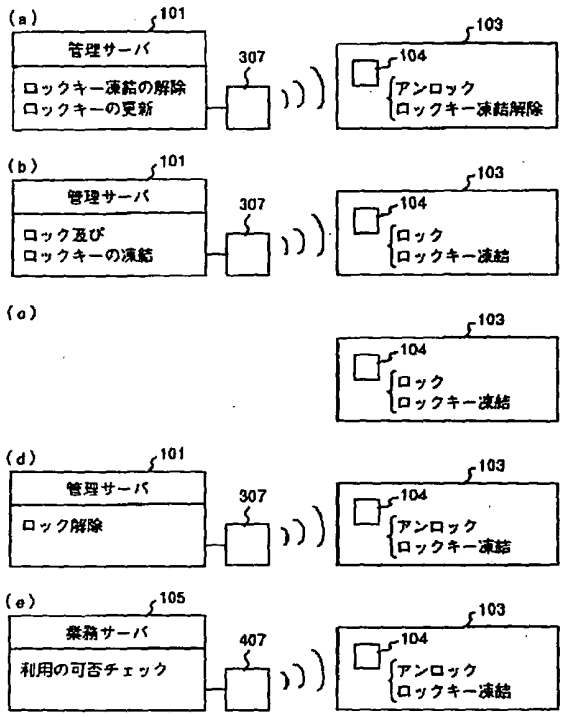
【図1】

図 1



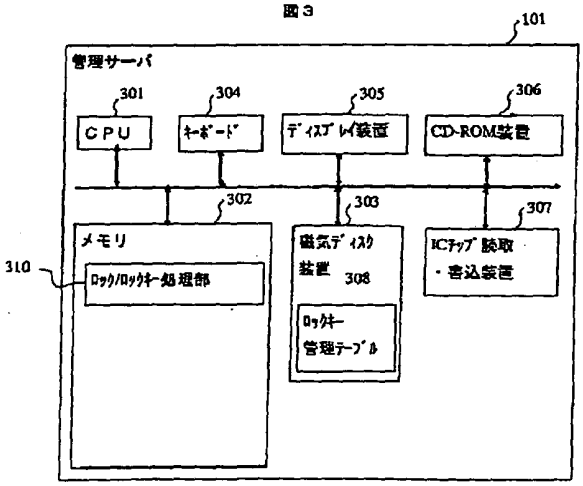
【図2】

図 2



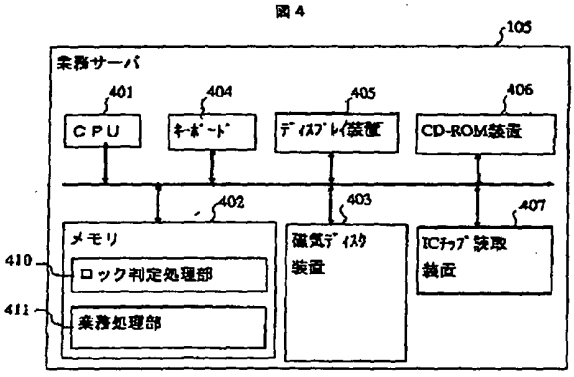
【図3】

図3



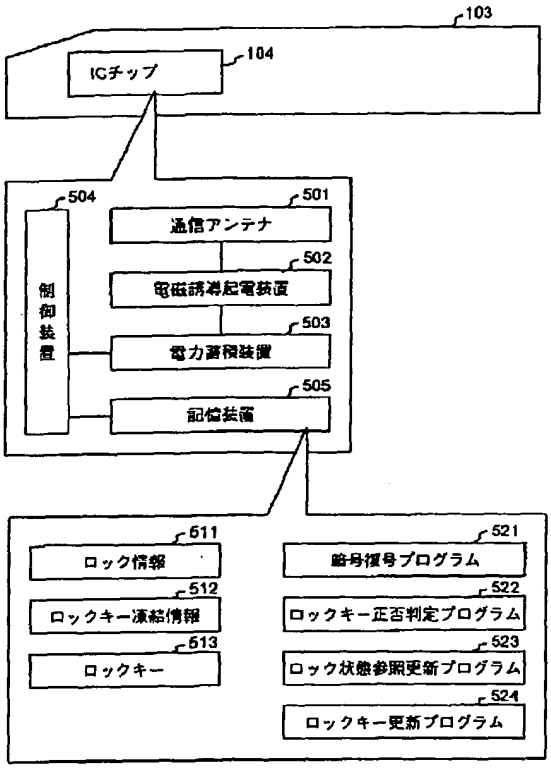
【図4】

図4



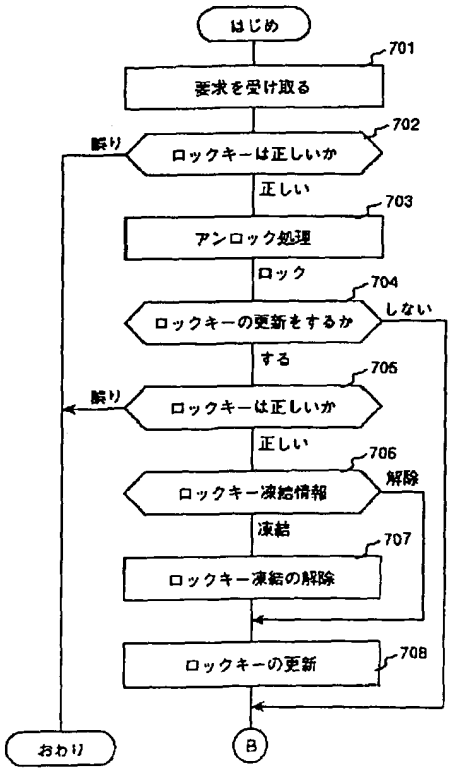
【図５】

図　5



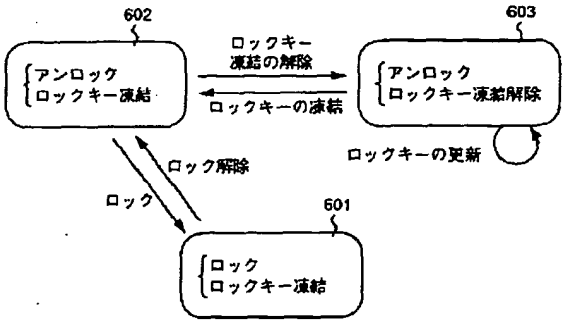
【図７Ａ】

図　7Ａ



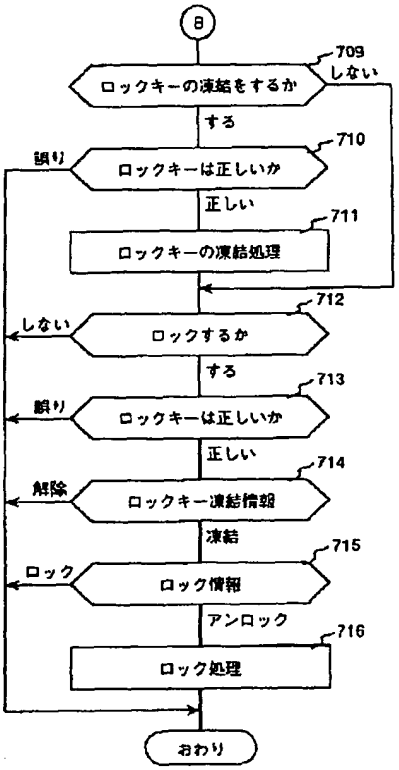
【図６】

図　6



【図７Ｂ】

図　7Ｂ



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
G06K	17/00	G06K	17/00	L 5B058
				F
	19/07	G07D	7/02	
	19/00	G06K	19/00	H
G07D	7/02			Q

Fターム(参考) 2C005 HA01 HA02 HB10 JA09 JB40
LB20 LB32 MA01 MA03 MA40
MB10 NA09 PA02 QA05 SA06
SA07 SA08
3E041 AA01 AA02 AA03 BA20 BB07
DB01
5B035 AA13 BA01 BB09 CA23
5B049 AA05 BB47 CC39 DD01 DD04
DD05 EE03 EE23 EE25 EE28
FF03 FF04 FF08 FF09 GG03
GG06 GG10
5B055 CC10 CC13 EE02 EE13 EE17
EE21 EE27 HA12 JJ05 KK05
KK09 KK18 PA02 PA34
5B058 CA15 KA01 KA31 KA35